

# ALGEBRAIC NUMBER FIELDS

(L-FUNCTIONS AND GALOIS PROPERTIES):

PROCEEDINGS OF A SYMPOSIUM

ALBRECHT FRÖHLICH

ACADEMIC PRESS

# Algebraic Number Fields

(L-functions and Galois properties)

Proceedings of a Symposium organised by the London Mathematical Society with the support of the Science Research Council and the Royal Society

Edited by

A. FRÖHLICH

*King's College, University of London*

1977



ACADEMIC PRESS

London: New York: San Francisco

*A Subsidiary of Harcourt Brace Jovanovich, Publishers*



ACADEMIC PRESS INC. (LONDON) LTD.  
24/28 Oval Road,  
London NW1

*United States Edition published by*  
ACADEMIC PRESS INC.  
111 Fifth Avenue  
New York, New York 10003

Copyright ©1977 by  
ACADEMIC PRESS INC. (LONDON) LTD.

*All Rights Reserved*

No part of this book may be reproduced in any form by photostat, microfilm, or any other means, without written permission from the publishers

Library of Congress Catalog Card Number: 76-016966

ISBN: 0-12-268960-7

QA  
247  
.A5228

Printed in Great Britain by Galliard (Printers) Ltd, Great Yarmouth, Norfolk

## List of Contributors

C.J. Bushnell,  
Department of Mathematics,  
King's College London,  
Strand,  
London WC2R 2LS

W. Casselman,  
Department of Mathematics,  
University of British Columbia,  
2075 Westbrook Place,  
Vancouver, B.C.,  
Canada.

J. Coates,  
Department of Pure Mathematics and Mathematical Statistics,  
University of Cambridge,  
16 Mill Lane,  
Cambridge.

J. Cougnard,  
Mathématiques,  
Université de Besançon,  
Route de Gray - La Bouloie,  
25030 Besancon Cedex,  
France.

A. Fröhlich,  
Department of Mathematics,  
King's College London,  
Strand,  
London WC2R 2LS

H. Koch,  
ADW der DDR,  
ZI für Mathematik und Mechanik,  
DDR 108 Berlin,  
Mohrenstr. 39.

J.C. Lagarias,  
Bell Laboratories,  
Murray Hill, N.J. 07974,  
U.S.A.

J. Martinet,  
Department de Mathématiques,  
Université de Bordeaux,  
351 Cours de la Libération,  
33405 Talence,  
France.

J. Masley,  
Department of Mathematics,  
University of Illinois at Chicago Circle,  
Chicago, Ill. 60680,  
U.S.A.

L.R. McCulloh,  
Department of Mathematics,  
University of Illinois at Urbana,  
Urbana, Ill. 61801,  
U.S.A.

O. Neumann,  
DAW-Inst.-komplex Mathematik,  
IRM,  
DDR 1199 Berlin-Adlershof,  
Rudower Chaussee 5.

A.M. Odlyzko,  
Bell Laboratories,  
Murray Hill, N.J. 07974,  
U.S.A.

R. Odoni,  
Department of Mathematics,  
University of Exeter,  
North Park Road,  
Exeter EX4 4QE

J-P. Serre,  
Collège de France,  
Paris, France.

H. Stark,  
Department of Mathematics,  
MIT,  
Cambridge, Mass. 02139,  
U.S.A.

J. Tate,  
Department of Mathematics,  
Harvard University,  
1 Oxford Street,  
Cambridge, Mass. 02138,  
U.S.A.

M.J. Taylor,  
Department of Mathematics,  
King's College London,  
Strand,  
London WC2R 2LS

A.A. Terras,  
Department of Mathematics,  
University of California at San Diego,  
P.O. Box 109,  
La Jolla, Calif. 92037,  
U.S.A.

S.V. Ullom,  
Department of Mathematics,  
University of Illinois at Urbana,  
Urbana, Ill. 61801,  
U.S.A.

R.W. van der Waall,  
Mathematisch Instituut,  
Katholieke Universiteit,  
Toernooiveld,  
Nijmegen,  
Holland.

## Preface

This volume is the outcome of a symposium on L-functions and Galois properties of algebraic number fields, held from 2 to 12 September 1975, in the University of Durham. It was organised by the London Mathematical Society, with the generous financial support of the Science Research Council, aided further by a grant from the Royal Society. The smooth running of the conference was made possible by the helpful attitude of the authorities of Durham University and the hard work of the symposium secretary, Dr. S.M.J. Wilson.

Almost all the lectures given at the symposium are recorded here. In many cases the presentation has been expanded and new relevant material added. My gratitude is due to the lecturers for making publication of this volume possible by their willing cooperation, as well as for their original contribution to the success of the meeting itself.

I also wish to express my thanks to Mrs. J. Bunn, who typed the whole volume ready for publication, to Mrs. E. Smith, who edited the manuscripts, to Dr. J.C. Bushnell for help on all fronts and to Academic Press London for continued cooperation.

A. Fröhlich

# Contents

	Page
List of Contributors	v
Preface	ix
J. Martinet, Character theory and Artin L-functions.	1
J.T. Tate (prepared in collaboration with C.J. Bushnell and M. Taylor), Local constants.	89
A. Fröhlich, Galois module structure.	133
J-P. Serre (prepared in collaboration with C.J. Bushnell), Modular forms of weight one and Galois representations.	193
J. Coates, p-adic L-functions and Iwasawa's theory.	269
H.M. Stark, Class fields for real quadratic fields and L-series at 1.	355
A.M. Odlyzko, On conductors and discriminants.	377
J.C. Lagarias and A.M. Odlyzko, Effective versions of the Chebotarev density theorem.	409
J. Masley, Odlyzko bounds and class number problems.	465
A. Terras, A relation between $\zeta_K(s)$ and $\zeta_K(s-1)$ for algebraic number field K.	475

	Page
R. Odoni, Some global norm density results obtained from an extended Chebotarév density theorem.	485
S.V. Ullom, A survey of class groups of integral group rings.	497
J. Martinet, $H_8$ .	525
J. Cougnard, Un contre-exemple a une conjecture de J. Martinet.	539
L.R. McCulloh, A Stickelberger condition on Galois module structure for Kummer extensions of prime degree.	561
A. Fröhlich, Stickelberger without Gauss sums.	589
H. Koch, Fields of class two and Galois cohomology.	609
O. Neumann, On p-closed number fields and an analogue of Riemann's existence theorem.	625
R.W. van der Waall, Holomorphy of quotients of zeta-functions.	649
W. Casselman, $GL_n$ .	663

# Character theory and Artin L-functions

J. Martinet

## I. NON ABELIAN L-FUNCTIONS

The aim of this chapter is to describe the theory of Artin's non abelian L-functions, taking for granted the theory of abelian L-functions. This chapter owes much to a talk by Serre (Fonctions L non abéliennes, Séminaire de Théorie des Nombres, Bordeaux, 10 avril 1973).

### §1. Frobenius

Two papers of Frobenius, both dating back to 1896, play a key role in the theory we are going to describe. The first one is devoted to what is now called the "Frobenius substitution". Let  $E/K$  be a finite normal extension of number fields with Galois group  $G$ , and let  $\mathfrak{p}$  be a finite prime of  $K$ . Assume  $E/K$  is unramified at  $\mathfrak{p}$ . For every prime  $P$  of  $E$  lying above  $\mathfrak{p}$ , there is a unique element  $\sigma_P \in G$  (the



Frobenius substitution) such that, for any integral  $x \in E$ , the congruence  $\sigma_P(x) \equiv x^{N(p)} \pmod{P}$  holds, where  $N(p)$  is the absolute norm of  $p$ . Moreover, the conjugacy class of  $\sigma_p$  in  $G$  does not depend on the particular choice of  $P$  above  $p$  in  $E$ . Frobenius stated in this paper a density theorem of the Čebotarev type, and proved the following result: for every cyclic subgroup  $C$  of  $G$ , there exist infinitely many primes  $P$  such that  $\sigma_P$  is a generator of  $C$ . Even disregarding questions of density, this is weaker than Čebotarev's theorem which asserts that every generator of  $C$  is of the form  $\sigma_P$  for infinitely many  $P$ .

The second paper of Frobenius we are concerned with is devoted to the definition of the characters. As will be seen in a moment, the theory of L-functions relies heavily on the consideration of both the notion of a character and of the Frobenius substitution. But Frobenius did not see the connection, and the sequel of his work deals mainly with the theory of characters.

## §2. Weber

For an ideal  $\mathfrak{f}$  of  $K$ , let  $I_{\mathfrak{f}}$  be the group of ideals of  $K$  prime to  $\mathfrak{f}$  and let  $P_{\mathfrak{f}}$  be the subgroup of  $I_{\mathfrak{f}}$  which consists

of ideals which can be generated by a totally positive element  $\alpha$  of  $K$  congruent to 1 mod  $\mathfrak{f}$ . Let  $H$  be a subgroup of  $I_{\mathfrak{f}}$  containing  $P_{\mathfrak{f}}$  (we call such a subgroup a congruence subgroup).

Weber called an abelian extension  $E$  of  $K$  "a class field for  $H$ " if the prime ideals of  $K$  which decompose completely in  $E$  are precisely those which belong to  $H$ , and if  $\mathfrak{f}$  is in some sense the smallest possible ideal. In this situation, the prime divisors of  $\mathfrak{f}$  are precisely the prime ideals of  $K$  which are ramified in  $E$ .

Now, for every character  $\chi : I_{\mathfrak{f}}/H \rightarrow \mathbb{C}^*$ , there is an L-function defined for  $\text{Re}(s) > 1$  by:

$$L(s, \chi) = \prod_{p \nmid \mathfrak{f}} \frac{1}{1 - \chi(p) N(p)^{-s}}.$$

The question arises of comparing the zeta function  $\zeta_E(s)$  with the product  $\prod L(s, \chi)$  when  $E$  is a class field for  $H$ . Generally, they are not equal, because of the possible existence of prime ideals which are ramified in  $E/K$  but not in the subfield corresponding to the kernel of  $\chi$ . I shall write

$$\zeta_E(s) \sim \prod_{\chi} L(s, \chi)$$

to mean that the equality is true up to a finite number of factors.

To obtain an equality, one must, for each character  $\chi$ , replace  $\mathfrak{f}$  by the conductor of  $\chi$ . This was known to Weber for those abelian extensions which were known to be class fields.

### §3. Artin's first definition of L-functions

Artin's first definition of L-functions appeared in 1922 (on a new kind of L series). In the meantime (1920) Takagi had established in full generality the classical results of class field theory, namely the one-to-one correspondence between abelian extensions of number fields and congruence subgroups, and also the isomorphism theorem, which asserts that the Galois group  $G$  of the extension is isomorphic to the quotient  $I_{\mathfrak{f}}/H$ .

Using an isomorphism between  $I_{\mathfrak{f}}/H$  and  $G$ , it would be possible to define L-functions for degree one characters of  $G$ . But Takagi's theory does not give any canonical isomorphism between  $I_{\mathfrak{f}}/H$  and  $G$ . Nevertheless, Artin thought that the L-series we defined previously with a congruence class character could be identified with L-series defined for a degree one character  $\psi$  of  $G$  by the formula:

$$L(s, \psi) = \prod_{\substack{p \\ \text{unramified}}} \frac{1}{1 - \psi(\sigma_p) N(p)^{-s}}$$

where  $\sigma_p$  is the Frobenius substitution of one  $P$  above  $p$  (Note that  $\sigma_p$  is well defined since  $G$  is abelian). This led Artin to conjecture that one obtains an isomorphism between  $I_f/H$  and  $G$  by sending the class in  $I_f/H$  of an unramified prime ideal  $p$  onto the Frobenius substitution  $\sigma_p$ . This Artin called "the general law of reciprocity" (because it implies fairly easily the known laws of reciprocity). In his paper on L-functions, he proves the law of reciprocity for a lot of abelian extensions  $E/K$  (e.g. cyclotomic extensions, cyclic extensions of prime power degree  $p^n$  when  $K$  contains the  $p^n$ -th roots of unity, cyclic extensions of prime degree, ...). He was quite sure of the validity of his reciprocity law. Indeed, it is stated as a theorem (Satz), and his paper of 1927 on the reciprocity law is simply called "proof of the general reciprocity law".

We are now able to give Artin's first definition of L-functions:

Definition Let  $E/K$  be a finite normal extension of number fields with Galois group  $G$ . Let  $V$  be a finite dimensional complex vector space, and let  $s \mapsto \rho(s)$  be a representation of  $G$  in  $V$ . Denote by  $\chi$  the character of  $\rho$ , defined by

$\chi(s) = \text{Tr}(\rho(s))$  for all  $s \in G$ . For a prime  $p$  in  $K$ , the determinant  $\det(1 - N(p)^{-s} \rho(\sigma_p))$  does not depend on the choice of  $P$  above  $p$ , and takes the same value for two isomorphic representations. We can therefore define

$$L(s, \chi) = \prod_{\substack{p \\ \text{unramified}}} \frac{1}{\det(1 - \rho(\sigma_p) N(p)^{-s})} .$$

The series is convergent for  $\text{Re}(s) > 1$ .

It is then obvious that  $L$  is additive, i.e. :

$$(a) \quad L(s, \chi_1 + \chi_2) = L(s, \chi_1) L(s, \chi_2) .$$

The following equalities, however, are true only up to a finite number of Euler-factors (we use the notation " $\sim$ ").

Let  $H$  be a normal subgroup of  $G$  corresponding to an extension  $F/K$ . Let  $\rho$  be a representation of  $G/H$  with character  $\chi$  and let  $\rho'$  be the lifting of  $\rho$  to  $G$  with character  $\chi'$ . Then we have the lifting formula

$$(b) \quad L(s, \chi') \sim L(s, \chi) .$$

Let  $H$  be a subgroup of  $G$ , and let  $\chi$  be a character of  $H$  which induces the character  $\chi^*$  of  $G$ . Then we have the induction formula

$$(c) \quad L(s, \chi^*) \sim L(s, \chi) .$$

Moreover, Artin proved that  $L(s, 1) \sim \zeta_K(s)$ .

Applying formula (c) to the unit character of a subgroup  $H$  of  $G$  corresponding to an extension  $F/K$ , we obtain the formula  $\zeta_F(s) \sim L(s, r_{G/H})$ , where  $r_{G/H}$  is the character of the permutation representation of  $G$  on  $G/H$ .

Let us take  $H = (1)$  in the above formula. Then  $r_{G/H}$  is the character  $r_G$  of the regular representation of  $G$ , which is just the sum  $\sum_{\chi} \chi(1)\chi$  over all irreducible characters of  $G$ . Now applying formula (a), we get

$$\zeta_E(s) \sim \prod_{\chi \text{ irreducible}} L(s, \chi)^{\chi(1)}.$$

Assuming the reciprocity law, Artin gave a proof of the theorem of density conjectured by Frobenius. He stated the existence of an analytic continuation for his  $L$  functions (with perhaps "ramification" points) and of a functional equation relating  $L(s, \chi)$  and  $L(1-s, \bar{\chi})$  as had been proved in 1917 by Hecke for abelian  $L$ -functions. He also asked whether his  $L$  functions are holomorphic in the whole complex plane for a character which does not contain the unit character. We now call this statement "the Artin conjecture".

#### §4. The general definition of non abelian $L$ -functions

Surprisingly, Čebotarev proved in 1926 the density theorem conjectured by Frobenius without using  $L$ -functions.



The main idea behind the proof is to reduce to the case of a cyclotomic extension. In 1927, using this device, Artin proved his general law of reciprocity. In 1930, he returned to the problems of L-functions in his paper "on the theory of L series with general characters". The two main problems are:

(i) To define local factors at ramified primes, in such a way as to put true equalities in the above formulae.

(ii) To define local factors at infinity and an exponential factor in order to get an analytic continuation and a functional equation.

(i) As always, we consider a normal extension  $E/K$  of number fields with Galois group  $G$  and a complex representation  $\rho : G \rightarrow \text{Gl}(V)$  with character  $\chi$ . Let  $\mathfrak{p}$  be a prime of  $K$ ; choose a prime  $P$  above  $\mathfrak{p}$ . Let  $D_P$  and  $I_P$  denote, respectively, the decomposition group and the inertia group of  $P$ . Now, the quotient group  $D_P/I_P$  is isomorphic to the Galois group of the residue extension. Hence, we can define a Frobenius substitution  $\sigma_P$  belonging to  $D_P/I_P$ . The vector space  $V$  is acted on by  $G$  via the formula  $\sigma x = \rho_\sigma(x)$  for all

$x \in V$  and all  $\sigma \in G$ . Let

$$V^{I_P} = \{x \in V \mid \forall \sigma \in I_P, \sigma x = x\},$$

the subspace of elements of  $V$  fixed by  $I_P$ . Once more, the determinant of the transformation  $(1 - N(p)^{-s} \sigma_p)$  of  $V^{I_P}$  does not depend on the particular choice of  $P$  above  $p$ , and is the same for two isomorphic representations. We can thus define

$$L(s, \chi) = \prod_{\substack{p \\ \text{finite}}} \frac{1}{\det_{V^{I_P}} (1 - N(p)^{-s} \sigma_p)}$$

for  $\text{Re}(s) > 1$ .

Now, the induction formula and the lifting formula become equalities. We summarize the fundamental results (notation as above):

- Theorem
- (a)  $L(s, \chi_1 + \chi_2) = L(s, \chi_1) L(s, \chi_2)$
  - (b)  $L(s, \chi') = L(s, \chi)$
  - (c)  $L(s, \chi^*) = L(s, \chi)$ .

Assume  $G$  is abelian. Let  $\chi$  be a degree one character of  $G$ , and let  $\psi$  be the corresponding congruence class character. Then,

- (d)  $L(s, \chi) = L(s, \psi)$ .



An obvious corollary is the equality:

$$\zeta_E(s) = \prod_{\substack{\chi \\ \text{irreducible}}} L(s, \chi)^{\chi(1)}.$$

Moreover, if  $V$  is of dimension 1 and if  $\rho(I_P)$  does not act trivially, then  $V^{I_P} = (0)$ . This explains why, for an abelian  $L$  function, local factors corresponding to the primes dividing the conductor reduce to 1.

Artin gave a more explicit description of his functions using an expansion of  $\log L(s, \chi)$ . Let us first consider the case of an unramified prime  $p$  of  $K$ . Let  $d$  be the dimension of  $V$ , and let  $\lambda_i(p)$  ( $1 \leq i \leq d$ ) be the eigenvalues of  $\rho(\sigma_P)$  for some  $P$  above  $p$ . Then,

$$\det(1 - N(p)^{-s} \rho(\sigma_P)) = \prod_{i=1}^d (1 - \lambda_i(p) N(p)^{-s}).$$

Thus,

$$\begin{aligned} \log \frac{1}{\det(1 - N(p)^{-s} \rho(\sigma_P))} &= \sum_{i=1}^d \sum_{m=1}^{\infty} \frac{\lambda_i(p)^m}{m N(p)^{ms}} \\ &= \sum_{m=1}^{\infty} \frac{\chi(\sigma_P^m)}{m N(p)^{ms}}. \end{aligned}$$

where  $\chi(\sigma_P^m)$  is just the trace of the  $m$ -th power of the Frobenius substitution. For a prime  $P$  with ramification index  $e$ , the above definition of  $\chi(\sigma_P^m)$  makes no sense, as  $\sigma_P$  belongs to  $D_P/I_P$ . We define however  $\chi(\sigma_P^m)$  as an average,

$\chi(\sigma_p^m) = \frac{1}{e} \sum_{s \mapsto \sigma_p^m} \chi(s)$ , where the sum is taken over the elements  $s$  of  $D_p$  which map onto  $\sigma_p^m$  in  $D_p/I_p$ .

The logarithmic expansion is now true for any prime  $p$  of  $K$ . Hence:

$$\log L(s, \chi) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(\sigma_p^m)}{m N(p)^{ms}},$$

a formula which gives an expansion for the logarithmic derivative of  $L(s, \chi)$ :

$$\frac{L'(s, \chi)}{L(s, \chi)} = - \sum_p \log(N(p)) \sum_{m=1}^{\infty} \frac{\chi(\sigma_p^m)}{N(p)^{ms}}.$$

Remark. Let us choose a fixed algebraic closure  $\bar{\mathbb{Q}}$  of  $\mathbb{Q}$ .

Then every number field  $K$  can be considered as a subfield of

$\bar{\mathbb{Q}}$ . Let  $\Omega_K$  be the (infinite) Galois group  $\text{Gal}(\bar{\mathbb{Q}}/K)$ . Then

property (b) of the above theorem shows that an L function

is attached to every finite dimensional complex representa-

tion of  $\Omega_K$  with open kernel. Such a representation has a

character, and we can define as usual virtual characters of

$\Omega_K$ . Then property (a) allows us to define an L function

$L(s, \chi)$  for every virtual character  $\chi$  of  $\Omega_K$ .

(ii) We are now going to define an enlarged L-function

$\Lambda$  of the form  $\Lambda(s, \chi) = A(\chi)^{s/2} \gamma_\chi(s) L(s, \chi)$ , and to prove for it the existence of a meromorphic continuation together with a functional equation  $\Lambda(s, \chi) = W(\chi) \Lambda(1-s, \bar{\chi})$  for some constant  $W(\chi)$  of absolute value 1. According to the known properties of abelian L-functions, we must define  $\Gamma$ -factors and the constant  $A(\chi)$ .

Let us begin with the  $\Gamma$ -factors. Put  $\gamma(s) = \pi^{-s/2} \Gamma(s/2)$ . We define  $\gamma_\chi$  as a product  $\gamma_\chi(s) = \prod_v \gamma_\chi^v(s)$ , where  $v$  ranges over the infinite places of  $K$ , and  $\gamma_\chi^v$ , the local factor at infinity, is defined in the following way: for  $v$  complex, we put  $\gamma_\chi^v(s) = [\gamma(s) \gamma(s+1)]^{\chi(1)}$ . Now, let  $v$  be a real place of  $K$ . To every place  $w$  of  $E$  above  $v$  corresponds a decomposition group (or inertia group)  $G(w) = \{s \in G \mid sw = w\}$  of order 1 or 2. The generator of  $G(w)$  plays the role of the Frobenius substitution, and is defined up to conjugacy by  $v$ . We write for  $V$  a direct sum decomposition  $V = V_v^+ \oplus V_v^-$  corresponding to the eigenvalues  $+1$  and  $-1$  of  $\rho(\sigma_w)$  for a fixed  $w$  above  $v$ , and we put

$$\gamma_\chi^v(s) = \gamma(s)^{\dim V_v^+} \gamma(s+1)^{\dim V_v^-}.$$

The definition of  $A(\chi)$  needs the notion of a conductor  $\mathfrak{f}(\chi)$  which must generalise the conductors of class field

theory defined for abelian characters. The theory of this conductor, now called the Artin conductor, is developed in the paper "The group theoretical structure of the discriminants of algebraic number fields", written at the end of the year 1930.

Let  $\mathfrak{p}$  a prime ideal of  $K$ . Choose a prime ideal  $P$  above  $\mathfrak{p}$ . Let  $G_i$  ( $i \geq 0$ ) be the corresponding ramification groups ( $G_0$  is the inertia group) and let  $g_i$  be the order of  $G_i$ . We define a rational number

$$n(\chi, \mathfrak{p}) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \text{codim } V^{G_i}$$

( $n(\chi, \mathfrak{p})$  is actually independent of the choice of  $P$  above  $\mathfrak{p}$ ).

Theorem (Artin)  $n(\chi, \mathfrak{p})$  is an integer.

Nowadays, this is proved using Brauer's induction theorem (see Serre, *Corps locaux*, chap. VI, §1-3. for a proof).

To prove this theorem, Artin reduced to the case  $G = G_1$ , using an argument of Speiser. Now,  $G_1$  is a  $p$ -group and it was known to Artin that every irreducible character of a  $p$ -group is induced by a character of degree one of some subgroup. As Artin had established induction

properties for  $n(\chi, p)$ , the proof was reduced to the case of degree one characters. He could then complete the proof using a theorem of Hasse, now known as Hasse-Arf theorem after its generalization by Arf.

For an unramified prime ideal  $p$ , one has  $n(\chi, p) = 0$ . Therefore, the formula

$$\mathfrak{f}(\chi, E/K) = \mathfrak{f}(\chi) = \prod_p p^{n(\chi, p)}$$

defines an ideal of  $K$ , which is known as the Artin conductor.

The constant  $A(\chi)$  is now defined by the formula

$$A(\chi) = |d_K|^{\chi(1)} N_{K/\mathbb{Q}}(\mathfrak{f}(\chi)) ,$$

where  $d_K$  is the absolute discriminant of  $K$ .

Theorem Let  $\Lambda$  be the "enlarged" L-function defined by the formula  $\Lambda(s, \chi) = A(\chi)^{s/2} \gamma_\chi(s) L(s, \chi)$  for  $\text{Re}(s) > 1$ . Then  $\Lambda$  possesses a meromorphic continuation in the whole complex plane, and satisfies the functional equation  $\Lambda(1-s, \chi) = W(\chi) \Lambda(s, \bar{\chi})$  for some constant  $W(\chi)$  of absolute value 1 (the so-called "Artin root number").

In the theorem,  $\bar{\chi}$  is the complex conjugate of  $\chi$ . If

$\chi$  is the character of a representation  $\rho : G \rightarrow \text{Gl}(V)$ ,  $\bar{\chi}$  is the character of the contragredient representation

$\bar{\rho} : G \rightarrow \text{Gl}(V^*)$  ( $V^*$  is the dual space of  $V$ ), defined by

$$\langle \bar{\rho}_s(f), x \rangle = \langle f, \rho_s^{-1}(x) \rangle \quad \text{for all } s \in G, \quad x \in V, \quad f \in V^*.$$

Artin could not prove the existence of a meromorphic continuation for the function  $\Lambda$ . The theorem was proved in 1947 by Brauer. We now give the proof.

We must first establish properties (a), (b), (c) for the enlarged L-functions. Properties (a) (additivity) and (b) (lifting property) are easily verified for the functions  $L$  and  $\gamma_\chi$ , as well as for the conductor  $f(\chi)$ . Thus, they are true for the constant  $A(\chi)$ , and hence for the function  $\Lambda$  (therefore, we can define  $\gamma_\chi(s)$ ,  $f(\chi)$ ,  $A(\chi)$  and  $\Lambda(s, \chi)$  for a virtual character of  $\Omega_K$ ). It is not difficult to show the invariance of  $\gamma_\chi$  under induction. For the Artin conductor, the formula is a bit more complicated. Let  $H$  be a subgroup of  $G$  with fixed field  $F$ , and let  $\chi$  be a character of  $H$ . The conductor of the character  $\chi^*$  of  $G$  induced by  $\chi$  is given by:

$$f(\chi^*) = D_{F/K}^{\chi(1)} N_{F/K}(f(\chi)), \quad \text{where } D_{F/K} \text{ is the discriminant of the extension } F/K.$$

A simple calculation using the transitivity formula for discriminants gives the equality  $A(\chi^*) = A(\chi)$ , and thus the



induction formula  $\Lambda(s, \chi^*) = \Lambda(s, \chi)$  for the enlarged L-function.

We now apply Brauer's induction theorem: there exist subgroups  $H_i$  ( $1 \leq i \leq n$ ) of  $G$ , degree one characters  $\chi_i$  ( $1 \leq i \leq n$ ) of  $H_i$  and rational integers  $n_i$  ( $1 \leq i \leq n$ ) for some  $n$  such that the following equality holds:

$$\chi = \sum_{i=1}^n n_i \chi_i^*.$$

We thus have, by properties (a) and (c):

$$\Lambda(s, \chi) = \prod_{i=1}^n \Lambda(s, \chi_i)^{n_i}.$$

For  $1 \leq i \leq n$ , let  $F_i$  be the fixed field of  $H_i$ ,  $H_i'$  the kernel of  $\chi_i$  and  $F_i'$  the fixed field of  $H_i'$ . The extensions  $F_i'/F_i$  are cyclic extensions with Galois group  $G_i = H_i/H_i'$ . Writing  $\chi_i'$  for the character of  $G_i$  defined by  $\chi_i$ , we then have, by property (b):

$$\Lambda(s, \chi_i) = \Lambda(s, \chi_i').$$

We now use Hecke's results. By composition with the Artin map, the characters  $\chi_i'$  define congruence class characters (or idèle class characters in modern language)  $\psi_i$  of  $F_i$ , and we know, by property (d), that the function  $L(s, \chi_i')$  is equal to  $L(s, \psi_i)$ . Now, given an abelian L-function  $L(s, \psi)$ , Hecke defined an enlarged function  $\Lambda'(s, \psi)$

by the formula

$$\Lambda'(s, \psi) = A'(\psi)^{s/2} \gamma'_{\psi}(s) L(s, \psi),$$

where  $A'(\psi) = |d_K|_{N_{K/\mathbb{Q}}}(\mathfrak{f}(\psi))$  and  $\gamma'_{\psi}(s)$  is a product of gamma factors of the form  $\gamma(s)$  or  $\gamma(s+1)$  depending on the behaviour of  $\psi$  at infinity. He proved the existence of a meromorphic continuation in the whole complex plane for  $\Lambda'$  together with a functional equation

$$\Lambda'(1-s, \psi) = W'(\psi) \Lambda'(s, \bar{\psi})$$

for some constant  $W'(\psi)$  of absolute value 1. Note that the analytic continuation of  $\Lambda'$  is in fact holomorphic when  $\psi$  is not the trivial character.

Now, given a degree one character  $\chi$  on the Galois group of a cyclic extension  $F'/F$  and its corresponding idèle class character  $\psi$ , Artin proved the equality of the "Artin" conductor  $\mathfrak{f}(\chi)$  and the conductor of  $\psi$  in the sense of class field theory. We thus have  $A(\chi) = A'(\psi)$ , and the equality of the gamma factors  $\gamma_{\chi}$  and  $\gamma'_{\psi}$ , is easily verified.

Going back to our previous notation, we have  $\Lambda(s, \chi_i!) = \Lambda'(s, \psi_i)$  for all  $s \in \mathbb{C}$  with  $\text{Re}(s) > 1$ . This implies the existence of the meromorphic continuation for  $\Lambda(s, \chi) = \prod_{i=1}^n \Lambda'(s, \psi_i)^{n_i}$  as well as the functional equation. Moreover, the equality  $W(\chi) = \prod_{i=1}^n W'(\psi_i)^{n_i}$  shows that  $W(\chi)$  is



of absolute value 1.

Corollary With the notation of §3, the following properties hold for the Artin root number:

$$(a) \quad W(\chi_1 + \chi_2) = W(\chi_1) W(\chi_2)$$

$$(b) \quad W(\chi') = W(\chi)$$

$$(c) \quad W(\chi^*) = W(\chi).$$

Note that properties (a) and (b) allow us to define  $W(\chi)$  for a virtual character of  $\Omega_K$ .

#### §5. Some elementary remarks on the Artin conjecture

Recall that the Artin conjecture is the following: for a character  $\chi$  of a representation which does not contain the unit representation, the corresponding function  $L(s, \chi)$  (or, which amounts to the same, the enlarged function  $\Lambda(s, \chi)$ ) is holomorphic.

Artin's conjecture is true for characters of degree one (this is a consequence of Hecke's results for abelian L-functions). As we know that an L-function is meromorphic, it is enough to show that some power of it is holomorphic to prove Artin's conjecture. Thus, for a character  $\chi$  which is a linear combination with positive rational coefficients of

characters induced by non trivial degree one characters of subgroups, the corresponding L-function is holomorphic. Until recent work of Tate, this was the only way one could prove that a given L-function is holomorphic.\*

The following well known example is due to Aramata and was rediscovered by Brauer:

Example. Let  $E/K$  be a normal extension. Then the augmentation representation of its Galois group (the regular representation minus the unit representation) has the above property. Consequently, the quotient  $\zeta_E(s)/\zeta_K(s)$  is holomorphic, or, as one says,  $\zeta_K(s)$  divides  $\zeta_E(s)$ .

Note that it is not known whether  $\zeta_K(s)$  divides  $\zeta_E(s)$  if  $E/K$  is not assumed to be normal. The result, however, would follow from a proof of Artin's conjecture.⊗

---

\*Footnote: But see a recent paper of Langlands mentioned in Serre's talk (3.3)).

⊗Footnote: See here also Van der Waall's talk.

## REFERENCES (CHAPTER I)

- E. Artin, Über eine neue Art von L-Reihen, Hamb. Abh., 1 (1923), 89-108, Collected papers n° 3.
- E. Artin, Beweis des allgemeinen Reziprozitätsgesetzes, Hamb. Abh., 5 (1927), 353-363, Collected papers n° 5.
- E. Artin, Zur Theorie der L-Reihen mit allgemeinen gruppencharakteren, Hamb. Abh., 8 (1930), 292-306, Collected papers n° 8.
- E. Artin, Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, J. Reine angew. Math., 164 (1931), 1-11, Collected papers n° 9.
- R. Brauer, On Artin's L series with general group characters, Ann. of Math. (2) 48 (1947), 502-514.
- N. Čebotarev, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebene Substitutionsklasse gehören, Math. Ann., 95 (1925), 191-228.
- F.G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Zahlkörpers und den Substitutionen seiner Gruppe, Gesammelte Abhandlungen, Bd II, n° 52, 719-733.
- F.G. Frobenius, Über gruppencharaktere, Gesammelte Abhandlungen, Bd III, n° 53, 1-37.
- E. Hecke, Über die L-functionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper, Nachrichten Göttingen (1917), 299-318, Werke, n° 9.
- R.P. Langlands, Base change for  $GL(2)$  (Lecture notes, IAS Princeton, 1975).
- J-P. Serre, Modular forms of weight one and Galois representation, Durham Symposium.
- R.W. van der Waall, Holomorphy of quotients of Zeta functions, Durham Symposium.

## II. GALOIS ACTION ON ROOT NUMBERS

This chapter is devoted to Galois Gauss sums. The main result is a theorem of Fröhlich, which gives a formula for the Galois action on the Galois Gauss sum, and hence on the root number. Fröhlich proved his theorem by global methods, and the proof I gave in Durham closely followed his original proof. I give here a local version of this theorem, from which the global result is easily deduced. This has been made possible by the theory of local constants of Langlands and Deligne.

§1. More on the Artin conductor

The Artin conductor can be defined for more general extensions than extensions of number fields. Let  $A$  be a Dedekind ring and  $K$  its quotient field. Let  $E$  be a finite normal extension of  $K$  with Galois group  $G$ , and let  $\rho$  be a representation of  $G$  in a finite dimensional vector space with character  $\chi$ . Assume that all the residue class extensions are separable. Let  $\mathfrak{p}$  be a prime ideal of  $K$ . Let us choose

a prime ideal  $P$  in  $E$  above  $p$ . We can then define the ramification groups  $G_i$  of  $P$ . Writing  $g_i$  for the order of  $G_i$ , we define as in chapter I,

$$n(\chi, p) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \operatorname{codim} V^{G_i}.$$

Theorem 1.1.  $n(\chi, p)$  is an integer.

(For a proof, see Serre, Corps Locaux, chap. VI, §1-3).

In particular, if  $E/K$  is unramified at  $p$ , then

$n(\chi, p) = 0$ , and if  $E/K$  is tamely ramified, then  $n(\chi, p) = \operatorname{codim} V^{G_0}$ .

We now define the Artin conductor by the formula:

$$\mathfrak{f}(\chi) = \prod_p p^{n(\chi, p)}.$$

The Artin conductor has the following 3 fundamental properties:

$$(a) \quad \mathfrak{f}(\chi + \chi') = \mathfrak{f}(\chi) \cdot \mathfrak{f}(\chi')$$

(b) If  $\chi$  is lifted from a character  $\chi'$  of a quotient  $H$  of  $G$ , then:

$$\mathfrak{f}(\chi) = \mathfrak{f}(\chi').$$

(c) Let  $H$  be a subgroup of  $G$ , corresponding to a subfield  $F$  of  $E$ ; let  $\chi$  be a character of  $H$  and let  $\chi^*$  be the character of  $G$  induced by  $\chi$ . Then:

$$\delta(\chi^*) = N_{F/K}(\delta(\chi)) \cdot D(F/K)^{\chi(1)}$$

where  $D(F/K)$  is the discriminant (relative to the ring  $A$ ) of the extension  $F/K$ .

Let  $D_P$  be the decomposition group of some ideal  $P$  above  $p$ , and let  $\chi_P$  be the restriction of  $\chi$  to  $D_P$ . Then  $\chi$  is induced by  $\chi_P$ . Let  $E_{(P)}$  be the decomposition field of  $P$ . Then,  $E_{(P)}/K$  is unramified, and formula (c) shows the equality:

$$n(\chi, p) = n(\chi_P, P \cap E_P).$$

Let  $\hat{E}_P$  (resp.  $\hat{K}_P$ ) be the completion of  $E$  (resp.  $K$ ) at  $P$  (resp.  $p$ ). Then  $D_P$  is canonically isomorphic to the Galois group of  $\hat{E}_P/\hat{K}_P$ , and the integer  $n(\chi, p)$  is the corresponding integer  $n(\chi_P, \hat{p})$  defined for this extension.

When  $A$  is a discrete valuation ring, there is no need to specify the ideal we choose, and we simply write  $n(\chi)$  instead of  $n(\chi, p)$ .

We now restrict ourselves to the case when  $K$  is a number field, and we define an integer  $n(\chi, v)$  for every infinite place  $v$  of  $K$ . If  $v$  is complex, then so is every place of  $E$  above  $v$ ; we say in this case that  $E/K$  is unramified at  $v$ , and simply put  $n(\chi, v) = 0$ .

If  $v$  is real, let  $w$  be a place of  $E$  above  $v$ . In Chapter I, we defined the "inertia group"  $I_w = \{s \in G \mid sw = w\}$ . We consider that the extension  $E/K$  is tamely ramified at  $v$ , and we define  $n(\chi, v)$  by the formula:

$$n(\chi, v) = \text{codim } V^{\overset{I}{w}}.$$

Of course,  $n(\chi, v)$  does not depend on the choice of  $w$  above  $v$ , and  $n(\chi, v) = 0$  if  $w$  is real. We can use the decomposition  $V = V_v^+ \oplus V_v^-$  of  $V$  given in chapter I, §4. to compute  $n(\chi, v)$ . Clearly,  $n(\chi, v)$  is the number of eigenvalues equal to  $-1$  for a "real Frobenius"  $\sigma_v$ . Now,  $\chi(\sigma_v) = \dim V_v^+ - \dim V_v^-$ ; the following formula holds:

$$n(\chi, v) = \frac{1}{2} (\chi(1) - \chi(\sigma_v)).$$

Remark 1. The integer  $n(\chi, v)$  was used by Hasse to define the infinite components of the Artin conductor.

Remark 2. The same arguments can be used to compute  $n(\chi, p)$  for an extension which is tamely ramified at  $p$ :  $n(\chi, p)$  is the number of eigenvalues other than  $+1$  for a generator  $\sigma_p$  of the inertia group of some ideal  $P$  above  $p$ .

We can also define an integer  $n(\chi)$  in the local archimedean case. Then,  $E$  and  $K$  are isomorphic either to



the field  $\mathbb{R}$  of real numbers or to the field  $\mathbb{C}$  of complex numbers, and we define  $n(\chi)$  by the formula:

$$n(\chi) = \text{codim } V^G.$$

Now, given a normal extension  $E/K$  of number fields, a place  $v$  of  $K$  and a character  $\chi$  on  $G = \text{Gal}(E/K)$ , one can define a local character  $\chi_v$  on  $\text{Gal}(E_w/K_v)$ , where  $K_v$  is the completion of  $K$  at  $v$  and  $E_w$  is the completion of  $E$  at some place  $w$  of  $E$  above  $v$ .

The situation is now the same as in the finite case, and the following equality holds:

$$n(\chi, v) = n(\chi_v) .$$

The proof is clear from the formulae  $n(\chi, v) = \frac{1}{2} (\chi(1) - \chi(\sigma_v))$  and  $n(\chi_v) = \frac{1}{2} (\chi_v(1) - \chi_v(\sigma_v))$ , since  $\chi_v$  is the restriction of  $\chi$  to the subgroup  $(1, \sigma_v)$  of  $G$ .

We end this § with the definition of the conductor for an infinite extension. We again use the definitions of the beginning of this section. Let  $L$  be an infinite normal extension of  $K$  with Galois group  $G$ . By a representation  $\rho$  of  $G$ , we understand a homomorphism  $\rho$  of  $G$  into the linear group of a finite complex vector space with open kernel. Such a representation factors through the Galois group of a finite extension. Recalling the invariance of the conductor



under lifting, we define  $\delta(\rho)$  to be the conductor of  $\rho'$ , where  $\rho'$  is any representation of a finite Galois extension such that  $\rho'$  lifts to  $\rho$  on  $G$ . Such a representation has a character  $\chi$ , and we can define  $n(\chi)$  as above. Virtual characters are then defined in the usual way, and the definition of the conductor of a virtual character is immediate.

Remark We define an unramified (virtual) character as a character which is the difference of 2 unramified characters of representations. It is clear that such a character has a trivial conductor. The converse however is false, for the difference of two ramified characters can well have a trivial conductor.

Thus unramified characters are the characters which can be factored through a finite unramified extension. In the same way, we define a tame character to be a character which factors through a finite tame extension.

## §2. Local Gauss sums

In this section,  $p$  is a fixed prime number and  $K$  a finite extension of the field  $\mathbb{Q}_p$  of  $p$ -adic numbers. Let  $\mathcal{O}_K$  (resp.  $\mathfrak{p}_K$ ,  $\mathcal{D}_K$ ,  $U_K$ ) be the valuation ring of  $K$  (resp. the

maximal ideal of  $O_K$ , the different of the extension  $K/\mathbb{Q}_p$ , the group of units of  $O_K$ ). For any integer  $i \geq 0$ , let  $U_K^i$  be the subgroup of those units of  $K$  which are congruent to 1 modulo  $p_K^i$  (thus,  $U_K^0 = U_K$ ). We denote by  $\pi_K$  a uniformizing parameter of  $O_K$  ( $p_K = \pi_K O_K$ ).

We first define the non trivial additive character  $\psi : K \rightarrow \mathbb{C}^*$  as the composition of the following 4 maps:

$$K \xrightarrow{(1)} \mathbb{Q}_p \xrightarrow{(2)} \mathbb{Q}_p / \mathbb{Z}_p \xrightarrow{(3)} \mathbb{Q} / \mathbb{Z} \xrightarrow{(4)} \mathbb{C}^*, \quad \text{where:}$$

- (1) is the trace  $\text{Tr}_{K/\mathbb{Q}_p}$
- (2) is the canonical surjection
- (3) is the canonical injection which maps  $\mathbb{Q}_p / \mathbb{Z}_p$  onto the  $p$ -component of the divisible group  $\mathbb{Q} / \mathbb{Z}$
- (4) is the exponential map  $x \mapsto e^{2\pi i x}$ .

For every  $x \in \mathbb{Q}_p$ , there is a rational  $r$ , uniquely defined modulo 1, such that  $x - r \in \mathbb{Z}_p$ . Then  $\psi(x) = \psi(r) = e^{2\pi i r}$ .

The equality  $\psi(x+y) = \psi(x)\psi(y)$  shows that  $\psi(-x) = \psi(x)^{-1} = \overline{\psi(x)}$  for every  $x \in K$ . We also remark that  $\psi$  is trivial on the codifferent  $\mathcal{D}_K^{-1}$ , and that  $\mathcal{D}_K^{-1}$  is actually the greatest ideal of  $K$  on which  $\psi$  is trivial.

The following lemma will be used to establish a basic

property of Gauss sums.

Lemma 2.1. Let  $n \geq 0$  be an integer and let  $d$  be an element of  $\mathcal{O}_K^{-1} N(p_K)^{-n}$ . Let  $S$  be a set of representatives of  $\mathcal{O}_K$  modulo  $p_K^n$ . Then, the sum  $\lambda = \sum_{y \in S} \psi(yd)$  does not depend on the particular choice of  $S$ . Moreover,  $\lambda = N(p_K)^n$  if  $d \in \mathcal{O}_K^{-1}$ , and  $\lambda = 0$  otherwise.

(For an ideal  $I$ ,  $N(I)$  denotes the unique power of  $p$  which generates the ideal  $N_{K/\mathbb{Q}_p}(I)$ ; if  $I$  is integral,  $N(I) = \text{card}(\mathcal{O}_K/I)$ ).

Proof If  $y' \equiv y \pmod{p_K^n}$ , then  $\psi(yd) \psi(y'd)^{-1} = \psi((y-y')d) = 1$ ; thus,  $\lambda$  does not depend on the choice of  $S$ . If  $d \in \mathcal{O}_K^{-1}$ , then  $\psi(yd) = 1$  and

$$\lambda = \sum_{y \in \mathcal{O}_K / p_K^n} 1 = N(p_K)^n.$$

Suppose now that  $d$  does not belong to  $\mathcal{O}_K^{-1}$ . For any integral  $z$ ,  $y+z$  runs through a full set of representatives of  $\mathcal{O}_K$  modulo  $p_K^n$  when  $y$  does. Thus  $\lambda = \sum_{y \in \mathcal{O}_K / p_K^n} \psi((y+z)d) =$

$\sum_{y \in \mathcal{O}_K / p_K^n} \psi(yd) \psi(zd) = \psi(zd) \lambda$ , and  $(1 - \psi(zd)) \lambda = 0$ . As  $\psi$  is not trivial on the ideal  $d\mathcal{O}_K$ , one can choose  $z$  such that  $\psi(zd) \neq 1$ . Hence,  $\lambda = 0$ .

Now let  $\theta: K^* \rightarrow \mathbb{C}^*$  be a character of  $K^*$  with open kernel.

Let  $n = n(\theta)$  be the valuation of the conductor  $f(\theta)$  of  $\theta$ , so that  $f(\theta) = p_K^n$ . The integer  $n$  is the least integer such that the character  $\theta$  is trivial on the group  $U_K^n$ .

We say that  $\theta$  is unramified if  $n(\theta) = 0$ . Then, for a non zero fractional ideal  $I$ , the value  $\theta(x)$  of  $\theta$  on a generator  $x$  of  $I$  does not depend on the choice of  $x$ ; we call it  $\theta(I)$ .

Definition The local Gauss sum  $\tau(\theta)$  is the sum

$$\tau(\theta) = \sum \theta\left(\frac{x}{c}\right) \psi\left(\frac{x}{c}\right),$$

where  $c$  is a generator of the ideal  $\mathcal{D}_\theta = f(\theta) \mathcal{D}_K$ , and  $x$  runs through a set of representatives of  $U_K$  modulo  $U_K^n$ .

When  $\theta$  is unramified, the sum reduces to 1 term, and we have the equality

$$\tau(\theta) = \theta(\mathcal{D}_K^{-1}).$$

If moreover  $K$  is an unramified extension of  $\mathbb{Q}_p$ , then  $\tau(\theta) = 1$ .

Remark It is easily verified that  $\tau(\theta)$  does not depend

on the choice of the representatives of  $U_K \bmod U_K^n$ . Hence,  $\tau(\theta)$  does not depend on the choice of  $c$ .

Proposition 2.2. Let  $\theta$  be a character of  $K^*$ . Then:

- (i)  $|\tau(\theta)| = \sqrt{N(f(\theta))}$
- (ii)  $\tau(\theta) \tau(\bar{\theta}) = \theta(-1) N(f(\theta)).$

Proof We first remark that (ii) is an easy consequence of (i), since

$$\begin{aligned} \tau(\bar{\theta}) &= \sum_x \bar{\theta}\left(\frac{x}{c}\right) \psi\left(\frac{x}{c}\right) = \sum_x \bar{\theta}\left(-\frac{x}{c}\right) \psi\left(-\frac{x}{c}\right) \\ &= \bar{\theta}(-1) \sum_x \bar{\theta}\left(\frac{x}{c}\right) \bar{\psi}\left(\frac{x}{c}\right) \\ &= \theta(-1) \overline{\tau(\theta)}. \end{aligned}$$

Moreover, if  $\theta$  is unramified, then  $N(f(\theta)) = 1$  and

$$\tau(\theta) \overline{\tau(\theta)} = \theta(\mathcal{D}_K^{-1}) \overline{\theta(\mathcal{D}_K^{-1})} = 1.$$

We now only have to prove (i) for a ramified character.

We write  $|\tau(\theta)|^2 = \tau(\theta) \overline{\tau(\theta)}$  as a double sum:

$$\tau(\theta) \overline{\tau(\theta)} = \sum_{x, y \in U_K / U_K^n} \theta\left(\frac{x}{c}\right) \psi\left(\frac{x}{c}\right) \bar{\theta}\left(\frac{y}{c}\right) \bar{\psi}\left(\frac{y}{c}\right).$$

Now,  $\bar{\theta}\left(\frac{x}{c}\right) = \theta^{-1}\left(\frac{x}{c}\right)$  and  $\bar{\psi}\left(\frac{x}{c}\right) = \psi\left(-\frac{x}{c}\right)$ ; replacing  $x$  by  $xy$ ,

we get the equality

$$\begin{aligned} \tau(\theta) \overline{\tau(\theta)} &= \sum_{x,y} \theta\left(\frac{xy}{c}\right) \theta^{-1}\left(\frac{y}{c}\right) \psi\left(\frac{xy}{c}\right) \psi\left(-\frac{y}{c}\right) \\ &= \sum_{x,y} \theta(x) \psi\left(y\left(\frac{x-1}{c}\right)\right) \\ &= \sum_x \theta(x) \phi(x), \text{ where} \end{aligned}$$

$$\phi(x) = \sum_{y \in U_K / U_K^n} \psi\left(y\left(\frac{x-1}{c}\right)\right).$$

We now write  $\phi(x)$  as the difference  $\sum_{y \in O_K / p_K^n} \psi\left(y\left(\frac{x-1}{c}\right)\right) -$

$$\sum_{y \in p_K / p_K^n} \psi\left(y\left(\frac{x-1}{c}\right)\right). \text{ By lemma 2.1., } \sum_{y \in O_K / p_K^n} \psi\left(y \frac{(x-1)}{c}\right) = 0$$

if  $x \not\equiv 1 \pmod{p_K^n}$ , and  $N(p_K)^n = N(\mathfrak{f}(\theta))$  otherwise; similarly,

$$\sum_{y \in p_K / p_K^n} \psi\left(y\left(\frac{x-1}{c}\right)\right) = \sum_{y \in O_K / p_K^{n-1}} \psi\left(y \frac{(x-1)\pi_K}{c}\right) = 0 \text{ if } x \not\equiv 1$$

$\pmod{p_K^{n-1}}$ , and  $N(p_K)^{n-1}$  otherwise. We thus have the

$$\text{equality } |\tau(\theta)| = N(\mathfrak{f}(\theta)) - \sum_{x \in U_K^{n-1} / U_K^n} \theta(x) N(p_K)^{n-1}, \text{ and we}$$

must prove that the sum  $\mu = \sum_{x \in U_K^{n-1} / U_K^n} \theta(x)$  is zero. But,

for any  $z \in U_K^{n-1}$ ,  $\theta(z) \mu = \sum_{x \in U_K^{n-1}/U_K^n} \theta(xz) = \mu$ . By the

definition of the conductor, there exist  $z \in U_K^{n-1}$  such that  $\theta(z) \neq 1$ . Hence,  $\mu = 0$ , Q.E.D.

We can now define the local root numbers. Let  $K$  be a local field of characteristic 0, and let  $\theta$  be a character of  $K^*$ .

Definition For  $K = \mathbb{R}$  or  $K = \mathbb{C}$ , define  $W(\theta) = i^{-n(\theta)}$ , where  $n(\theta)$  is the integer defined in section 1.

For  $K$  non archimedean, define  $W(\theta) = \frac{\tau(\bar{\theta})}{\sqrt{N(f(\theta))}}$ .

We now explain the connection between these local root numbers and the root number defined by Hecke for abelian  $L$  functions.

Let  $K$  be a number field, and let  $\chi$  be an idèle class character (i.e.,  $\chi$  is a continuous character on the group  $I_K$  of the idèles of  $K$ , trivial on the principal idèles). For every place  $v$  of  $K$ , the natural imbedding  $K_v^* \rightarrow I_K$  defines a character  $\chi_v$  on  $K_v^*$ . The following theorem was proved by Tate in 1950.



Theorem 2.3       $W(\chi) = \prod_v W(\chi_v).$

For a proof, see Tate's thesis, in Cassels-Fröhlich, p. 305-347. (Note that the infinite product makes sense because  $\tau(\chi_p) = N(\delta(\chi_p)) = 1$  for every finite prime  $p$  at which both the character  $\chi$  and the extension  $K/\mathbb{Q}$  are unramified).

### §3. The transfer

Given a group  $G$ , we denote by  $G^{ab}$  the quotient of  $G$  by its commutator subgroup. Let  $G$  be a group and let  $H$  be a subgroup of finite index in  $G$ . Let  $\theta : G/H \rightarrow H$  be a set of representatives for the left cosets of  $G$  modulo  $H$ . Given  $s \in G$  and  $t \in G/H$ , we define an element  $a_{s,t}$  of  $H$  by the formula:

$$s \theta(t) = \theta(st) a_{s,t}.$$

Definition      Let  $\bar{s} \in G^{ab}$ , and let  $s \in G$  be a representative of  $\bar{s}$ . The image in  $H^{ab}$  of the element  $\prod_{t \in G/H} a_{s,t}$  of  $H$  is called the transfer of  $\bar{s}$ .

Notation       $\text{Ver}_G^H(\bar{s})$  or simply  $\text{Ver}(\bar{s})$ ; we also define the transfer of  $s$  itself by  $\text{Ver}(s) = \text{Ver}(\bar{s})$ .

It can be shown that  $\text{Ver}(s)$  does not depend on the choices made in the definition, and that the transfer is a homomorphism of  $G^{\text{ab}}$  into  $H^{\text{ab}}$ . By duality, given an abelian group  $A$ , there is a transfer  $\text{Ver} : \text{Hom}(H, A) \rightarrow \text{Hom}(G, A)$ .

The transfer was first defined by Schur, and rediscovered by Artin in connection with class field theory. We shall use the transfer for its role in class field theory and for the calculation of the determinant of an induced representation.

a) Class field theory. For convenience, we use infinite Galois groups. For a topological group  $G$ , the group  $G^{\text{ab}}$  is the quotient of  $G$  by the closure of its commutator subgroup.

Proposition 3.1. The following two diagrams are commutative:

$$\begin{array}{ccc}
 \text{Gal}(\bar{\mathbb{Q}}_p/K)^{\text{ab}} & \xrightarrow{\text{Ver}} & \text{Gal}(\bar{\mathbb{Q}}_p/E)^{\text{ab}} \\
 \uparrow & & \uparrow \\
 K^* & \xrightarrow{\text{inclusion}} & E^*
 \end{array}$$

$$\begin{array}{ccc}
 \Omega_K^{\text{ab}} & \xrightarrow{\text{Ver}} & \Omega_E^{\text{ab}} \\
 \uparrow & & \uparrow \\
 I_K & \xrightarrow{\text{inclusion}} & I_E
 \end{array}$$

In both diagrams, the vertical maps are Artin maps.

In the left hand diagram,  $E/K$  is a finite extension of fields of finite degree over  $\mathbb{Q}_p$ , contained in a given algebraic closure  $\bar{\mathbb{Q}}_p$  of  $\mathbb{Q}_p$ .

In the right hand diagram,  $E/K$  is a finite extension of number fields, and  $I_K, I_E$  are the corresponding idèle groups.

We shall write  $\text{Ver}_{E/K}$  for the transfers involved in these 2 diagrams.

Proof This is a property of class formations (see e.g. Artin-Tate, Class Field Theory, chap. XIV, or Serre, Corps Locaux, chap. XI).

b) Induced representations. Given a representation  $\rho$  of a finite group  $G$  in a complex vector space  $V$ , the determinant of  $\rho$  depends only on the character of  $\rho$ . By linearity, we define the determinant of any virtual character  $\chi$  of  $G$ . (Notation :  $\det_\chi$ ).

Proposition 3.2. Let  $G$  be a finite group and let  $H$  be a subgroup of  $G$ . Let  $\chi$  be a character of  $H$ , and let  $\chi^*$  be

the character of  $G$  induced by  $\chi$ . For any element  $s \in G$ , let  $\epsilon_{G/H}(s)$  be the signature of the permutation of  $G/H$  defined by multiplication by  $s$ . Then:

$$\det_{\chi}^*(s) = \epsilon_{G/H}(s)^{\chi(1)} \det_{\chi}(\text{Ver}_G^H(s)) ,$$

or, more briefly:

$$\det_{\chi}^* = \epsilon_{G/H}^{\chi(1)} \cdot \text{Ver}(\det_{\chi}).$$

Proof By linearity, we may assume that  $\chi$  and  $\chi^*$  are characters of representations. Thus,  $\chi^*$  corresponds to a vector space  $V$  with  $G$  action, and  $\chi$  to a subspace  $W$  of  $V$  invariant under  $H$ . The fact that the representation afforded by  $V$  is induced by the representation afforded by  $W$  can be described in the following way. Let  $\theta = G/H \rightarrow G$  be a set of representatives of left cosets of  $G \bmod H$ . Let  $W_{\sigma} = \theta(\sigma) W$ . Then,  $V$  is the direct sum :  $V = \bigoplus_{\sigma \in G/H} W_{\sigma}$ . We must now find the determinant of the endomorphism  $x \mapsto sx$  of  $V$  for every  $s \in G$ .

Write  $x = \sum_{\sigma \in G/H} \theta(\sigma) x_{\sigma}$ , with  $x_{\sigma} \in W$ . Then,  $sx = \sum_{\sigma \in G/H} s \theta(\sigma) x_{\sigma} = \sum_{\sigma \in G/H} \theta(s\sigma) a_{s,\sigma} x_{\sigma}$ . Thus, the map  $x \mapsto sx$  is the product  $vu$ , where  $u$ , defined by  $\theta(\sigma)x_{\sigma} \mapsto \theta(\sigma)a_{s,\sigma}x_{\sigma}$ , maps each  $W_{\sigma}$  onto itself, and  $v$ , defined by

$\theta(\sigma) x_{\sigma} \mapsto \theta(s\sigma) \theta(\sigma)^{-1} x_{\sigma}$ , maps  $W_{\sigma} = \theta(\sigma) W$  onto  $\theta(s\sigma) W$ .

Now, everything is easy: first  $\det_V(u) = \prod_{\sigma \in G/H} \det_{W_\sigma}(u|_{W_\sigma})$   
 $= \prod_{\sigma} \det_W(x \rightarrow a_{s,\sigma} x) = \det_W(x \rightarrow \prod_{\sigma} a_{s,\sigma} x) = \det_{\chi}(\text{Ver}(s))$ . Now  
 let  $e_i (1 \leq i \leq \chi(1))$  be a basis of  $W$ . Consider the basis  
 $\theta(\sigma)e_i (\sigma \in G/H, 1 \leq i \leq \chi(1))$  of  $V$ . For each  $i$ ,  $v$  per-  
 mutes the  $\theta(\sigma)e_i$ , and the signature of the permutation is  
 $\varepsilon_{G/H}(s)$ . As there are  $\chi(1)$  indices  $i$ ,  $\det_V(v) =$   
 $\varepsilon_{G/H}(s)^{\chi(1)}$ , Q.E.D.

Corollary. If  $\chi$  is a character of trivial determinant and  
 of degree zero, so is the induced character  $\chi^*$ .

#### §4. Local Galois Gauss sums

Let  $p$  be a place of  $\mathbb{Q}$ , and let  $\bar{\mathbb{Q}}_p$  be an algebraic  
 closure of  $\mathbb{Q}_p$  (thus,  $\mathbb{Q}_\infty = \mathbb{R}$  and  $\bar{\mathbb{Q}}_\infty = \mathbb{C}$ ). By a local  
 field, we mean a finite extension of  $\mathbb{Q}_p$  which is contained  
 in  $\bar{\mathbb{Q}}_p$ . Given a local field  $K$ , we consider virtual char-  
 acters of  $\text{Gal}(\mathbb{Q}_p/K)$  which are differences of two characters  
 of representations of open kernel. We simply write  $G_K$  for  
 the Galois group  $\text{Gal}(\bar{\mathbb{Q}}_p/K)$ .

For a local field  $K$  and a (virtual) character  $\theta$  of  $G_K$ ,  
 Deligne and Langlands defined a local root number  $W(\theta)$  (see  
 Tate's lecture cf. [14]). The local root number is well

defined by the following three properties:

$$(i) \quad W(\theta_1 + \theta_2) = W(\theta_1) W(\theta_2).$$

(ii) Let  $\theta$  be a irreducible character of degree one, and let  $\theta^*$  be the character of  $K^*$  defined by  $\theta$  via the Artin map. Then,  $W(\theta)$  is the local root number  $W(\theta^*)$  defined in section 2.

(iii) Let  $E$  be a finite extension of  $K$ , let  $\theta$  be a character of degree zero of  $G_E$  and let  $\theta^*$  be the character of  $G_K$  induced by  $\theta$ . Then  $W(\theta^*) = W(\theta)$ .

We are now able to define the local Galois Gauss sum.

Definition Let  $K$  be a non archimedean local field, and let  $\theta$  be a character of  $\text{Gal}(\bar{\mathbb{Q}}_p/K)$ . The local Galois Gauss sum  $\tau(\theta)$  is defined by the formula:

$$\tau(\theta) = W(\bar{\theta}) \sqrt{N(f(\theta))},$$

where  $f(\theta)$  is the Artin conductor of  $\theta$  and the square root is the positive square root.

Note that  $f(\bar{\theta}) = f(\theta)$ . Hence

$$W(\theta) = \frac{\tau(\bar{\theta})}{\sqrt{N(f(\theta))}}.$$

The local Galois Gauss sum is well defined by the

following three properties which are obvious consequences of the corresponding properties for local root numbers and conductors:

$$(i) \quad \tau(\theta_1 + \theta_2) = \tau(\theta_1) \tau(\theta_2).$$

(ii) Let  $\theta$  be an irreducible character of degree one, and let  $\theta'$  be the character of  $K^*$  defined by  $\theta$  via the Artin map. Then,  $\tau(\theta) = \tau(\theta')$ , the local Gauss sum defined in section 2.

(iii) Let  $E$  be a finite extension of  $K$ , let  $\theta$  be a character of degree 0 of  $G_E$  and let  $\theta^*$  be the character of  $G_K$  induced by  $\theta$ . Then  $\tau(\theta^*) = \tau(\theta)$ .

Notation. Given a local field  $K$ , an element  $x \in K^*$  and an irreducible character of degree one  $\theta$  of  $G_K$ , we write  $\theta(x)$  for the element  $\theta(\omega)$ , where  $\omega \in G_K^{ab}$  is the image of  $x$  under the Artin map.

Proposition 4.1. Let  $K$  be a finite extension of  $\mathbb{Q}_p$ , and let  $\theta$  be a character of  $G_K$ . Then:

$$(i) \quad |\tau(\theta)| = \sqrt{N(\mathfrak{f}(\theta))}$$

$$(ii) \quad \tau(\theta) \tau(\bar{\theta}) = N(\mathfrak{f}(\theta)) \det_{\theta}(-1).$$

The following corollary is an easy consequence of the



above proposition for an extension of  $\mathbb{Q}_p$ , and is obvious for  $K = \mathbb{R}$  or  $K = \mathbb{C}$ :

Corollary. Let  $K$  be a local field. Then:

$$(i) \quad |W(\theta)| = 1$$

$$(ii) \quad W(\theta) W(\bar{\theta}) = \det_{\theta}(-1).$$

Proof. We have only to prove the proposition when  $\theta$  is an irreducible character of degree 1, and show that the 2 sides of the equalities are invariant under induction for characters of degree zero. Now, the case of an irreducible character of degree 1 has already been dealt with in §2, and both sides of the above equalities are invariant under induction when  $\theta$  is of degree 0 (for (ii), just remark that  $(\bar{\theta})^* = \bar{\theta}^*$ ).

Remark. Using part (ii) of proposition 4.1., one proves immediately the formula

$$W(\theta) \tau(\theta) = \det_{\theta}(-1) \sqrt{N(\theta(\theta))}.$$

§5. Galois action on Galois Gauss sums and root numbers  
(local theory)

Let  $K$  be local field, and let  $\theta$  be a character of  $G_K$ . The values of  $\theta$  are algebraic numbers. For any  $\omega \in \Omega_{\mathbb{Q}}$ , we define  $\theta^\omega$  by the formula:  $\theta^\omega(s) = (\theta(s))^\omega$  for every  $s \in G_K$ . We do not worry about left or right action of  $G_K$  as the results we are going to prove do not depend on the choice we make.

The aim of this section is to compute  $W(\theta^\omega)$  in terms of  $W(\theta)$  and the theorem we shall prove is just a local version of a global theorem of Fröhlich. For an archimedean local field,  $\theta^\omega = \theta$ , and there is nothing to do. We thus restrict ourselves to finite extensions of  $\mathbb{Q}_p$ ,  $p$  finite.

Now,  $\tau(\theta)$  is an algebraic number: for a character of degree one, this is clear from the definition, and the general case is a consequence of the induction formula. Therefore,  $W(\theta)$  itself is an algebraic number. We shall now compare  $\tau(\theta^\omega)$  with  $\tau(\theta)^\omega$ .

We first define a homomorphism  $u_p$  of  $\Omega_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  into  $U_p$ , the group of  $p$ -adic units.

Definition. Given  $\omega \in \Omega_{\mathbb{Q}}$ ,  $u_p(\omega)$  is the unique  $p$ -adic

unit such that  $\eta^{\omega^{-1}} = \eta^{u_p(\omega)}$ , for every  $p^n$ -th root of unity  $\eta$  in  $\bar{\mathbb{Q}}$ . For any extension  $K$  of  $\mathbb{Q}_p$ , we view  $u_p$  as a homomorphism of  $\Omega_{\mathbb{Q}}$  into  $K^*$ .

Theorem 5.1. Let  $K$  be a finite extension of  $\mathbb{Q}_p$  for some finite  $p$ , and let  $\theta$  be a character of  $G_K$ . Then, for any  $\omega \in \Omega_{\mathbb{Q}}$ ,

$$\tau(\theta^{\omega^{-1}})^{\omega} = \tau(\theta) \det_{\theta} (u_p(\omega)).$$

Proof. The proof is in 2 steps.

Step 1. Let  $\theta$  be a character of degree 0, and let  $F$  be a subfield of  $K$ . Assuming the formula is true for  $\theta$ , we prove it for the character  $\theta^*$  of  $G_F$  induced by  $\theta$ . For the right hand side, observe that  $\tau(\theta^*) = \tau(\theta)$  and that  $\det_{\theta^*}(u_p(\omega)) = \det_{\theta}(u_p(\omega))$  by propositions 3.1. and 3.2. . For the left hand side notice that  $(\theta^*)^{\omega^{-1}} = (\theta^{\omega^{-1}})^*$ , hence  $\tau(\theta^{*\omega^{-1}})^{\omega} = \tau((\theta^{\omega^{-1}})^*)^{\omega} = \tau(\theta^{\omega^{-1}})^{\omega}$ .

Step 2. We prove the formula for an irreducible character of degree 1. Regarding  $\theta$  as a character on  $K^*$ , we write,

with the notation of §2,  $\tau(\theta) = \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c}) \psi(\frac{x}{c})$ . Then:

$$\tau(\theta^{\omega^{-1}})^{\omega} = \sum_{x \in U_K/U_K^n} [\theta^{\omega^{-1}}(\frac{x}{c}) \psi(\frac{x}{c})]^{\omega} = \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c}) \psi(\frac{x}{c})^{\omega}.$$

Now,  $\psi(\frac{x}{c})$  is a  $p^n$ -th root of unity for some  $n$ . Thus,

$$\psi(\frac{x}{c})^{\omega} = \psi(\frac{x}{c})^{u_p(\omega^{-1})} = \psi(\frac{x}{c})^{u_p(\omega)^{-1}} = \psi(\frac{x}{c} u_p(\omega)^{-1}).$$

Therefore,

$$\begin{aligned} \tau(\theta^{\omega^{-1}})^{\omega} &= \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c}) \psi(\frac{x}{c} u_p(\omega)^{-1}) \\ &= \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c} u_p(\omega)) \psi(\frac{x}{c}) \quad (\text{by the transformation} \\ &\quad x \mapsto x u_p(\omega)) \\ &= \theta(u_p(\omega)) \tau(\theta) = \tau(\theta) \det_{\theta}(u_p(\omega)), \quad \text{Q.E.D.} \end{aligned}$$

We now state a corollary which is useful for the global theory. We defined a homomorphism  $u_p : \Omega_{\mathbb{Q}} \rightarrow U_p \subset \mathbb{Q}_p^*$ . By composition with the Artin map, we obtain a homomorphism  $v_p : \Omega_{\mathbb{Q}} \rightarrow \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)^{\text{ab}}$ .

Corollary 5.2. The notation being as in the theorem,

$$\tau(\theta^{\omega^{-1}})^{\omega} = \tau(\theta) \det_{\theta} (\text{Ver}_{K/\mathbb{Q}_p} (v_p(\omega))).$$

Proof. Obvious from the following commutative diagram:

$$\begin{array}{ccccc}
 & & \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)^{\text{ab}} & \xrightarrow{\text{Ver}} & \text{Gal}(\bar{\mathbb{Q}}_p/K)^{\text{ab}} \\
 & \nearrow V_p & \uparrow \text{Artin} & & \uparrow \text{Artin} \\
 \Omega_{\mathbb{Q}} & \xrightarrow{u_p} & \mathbb{Q}_p & \xrightarrow{\text{inclusion}} & K
 \end{array}$$

Remark 1. Let  $\omega'$  be an element in the inertia group of  $G_{\mathbb{Q}_p}^{\text{ab}}$ . As  $\Omega_{\mathbb{Q}}^{\text{ab}}$  is abelian, this element  $\omega'$  defines a unique element  $\omega \in \Omega_{\mathbb{Q}}^{\text{ab}}$  via any imbedding of  $\bar{\mathbb{Q}}$  in  $\bar{\mathbb{Q}}_p$ . To use the previous corollary, one must be able to compare  $\omega'$  and  $v_p(\omega)$ . The result is actually the following one:  
 $\omega' = v_p(\omega)$ . The equality is true thanks to the minus sign in the definition of  $u_p(\omega)$  (see Corps Locaux, last remark of chap. XIV, §7).

Remark 2. To finish this section, we come back to the root number itself. For any  $\omega \in \Omega_{\mathbb{Q}}$ ,  $f(\theta^{\omega}) = f(\theta)$ . Thus, using the formula  $W(\theta) = \frac{\tau(\bar{\theta})}{\sqrt{N(f(\theta))}}$ , we see that theorem 5.1 gives a way of computing  $W(\theta^{\omega})$  when  $f(\theta)$  and

$W(\theta)$  are known. To express the result in terms of  $W(\theta)$  itself, it is enough to know the action of  $\omega$  on  $\sqrt{N(f(\theta))}$ .

The following proposition is obvious:

Proposition 5.3. Let  $\theta$  be a character of  $G_K$  with trivial determinant. Assume that the norm of the conductor of  $\theta$  is a square. Then,  $W(\theta^\omega) = W(\theta)^\omega$ .

#### §6. Real valued characters

In this section,  $K$  is a local field and  $\theta$  a real valued character of  $G_K$ . The formula  $W(\theta) W(\bar{\theta}) = \det_\theta(-1)$  reduces to  $W(\theta)^2 = \det_\theta(-1)$ . Thus,  $W(\theta)$  is a fourth root of unity. Moreover, if  $\det_\theta$  is trivial, then  $W(\theta) = +1$  or  $-1$ .

The following two propositions give local versions of a global theorem of Fröhlich (see next section).

Proposition 6.1. Let  $K$  be a non archimedean local field, and let  $\theta$  a real valued character of  $G_K$  with trivial determinant. Each of the following conditions implies the other:

- (i)  $W(\theta^\omega) = W(\theta)$  for every  $\omega \in \Omega_{\mathbb{Q}}$

- (ii)  $\tau(\theta^\omega) = \tau(\theta)$  for every  $\omega \in \Omega_{\mathbb{Q}}$
- (iii)  $\tau(\theta)$  is a rational number.
- (iv)  $N(\mathcal{J}(\theta))$  is a square.

Proof. (i)  $\Rightarrow$  (ii). Since  $\bar{\theta} = \theta$ ,  $W(\theta) = \frac{\tau(\theta)}{\sqrt{N(\mathcal{J}(\theta))}}$ .

Since  $\mathcal{J}(\theta^\omega) = \mathcal{J}(\theta)$ ,  $\tau(\theta^\omega) = \tau(\theta) \frac{W(\theta^\omega)}{W(\theta)} = \tau(\theta)$ .

(ii)  $\Rightarrow$  (iii). By theorem 5.1.,  $\tau(\theta)^\omega = \tau(\theta^\omega) = \tau(\theta)$ .

(iii)  $\Rightarrow$  (iv).  $N(\mathcal{J}(\theta)) = \frac{\tau(\theta)^2}{W(\theta)^2} = \tau(\theta)^2$ .

(iv)  $\Rightarrow$  (i). Obvious by proposition 5.3.

Proposition 6.2. Let  $K$  be a non archimedean local field, and let  $\theta$  be a real valued character of  $G_K$ . Assume moreover that  $\theta$  is tame (i.e.,  $\theta$  factors through a finite tamely ramified extension). Then, the conductor of  $\theta$  is a square, and therefore  $W(\theta^\omega) = W(\theta)$  for every  $\omega \in \Omega_{\mathbb{Q}}$ .

Proof. We must prove that the integer  $n(\theta)$  is even. We can view  $\theta$  as a character of the Galois group of a finite tamely ramified extension  $E$  of  $K$ , and it is enough to give the proof when  $\theta$  is a character of a representation  $\rho$  of  $G$ . Now, we know that  $n(\theta)$  is the number of eigenvalues other



than +1 of  $\rho(\sigma)$ , where  $\sigma$  is a generator of the inertia group. Let  $n^-$  be the number of eigenvalues of  $\rho(\sigma)$  equal to -1. Since  $\theta$  is real valued, the non real eigenvalues appear in pairs of conjugates; hence,  $n(\theta) \equiv n^- \pmod{2}$ . Now, the determinant of  $\rho(\sigma)$  is the product of all eigenvalues of  $\rho(\sigma)$ . The product of the non real eigenvalues is +1. We thus have the equality  $+1 = \det(\rho(\sigma)) = (-1)^{n^-}$ . Hence,  $n(\theta) \equiv n^- \equiv 0 \pmod{2}$ , Q.E.D.

Remark. Let  $\theta$  be a character of a finite extension. The statement  $W(\theta^\omega) = W(\theta)$  for every  $\omega \in \Omega_{\mathbb{Q}}$  is equivalent to the following one : the value of  $W(\theta)$  depends only on the simple factor of  $\mathbb{Q}[G]$  corresponding to  $\theta$ . Another example where this situation arises will be given in chapter III, §4.

## §7. Global theory

In this section,  $K$  is a number field and  $\chi$  is a virtual character of the infinite Galois group  $\Omega_K = \text{Gal}(\bar{\mathbb{Q}}/K)$  which factors through a finite extension of  $K$ .

The Galois Gauss sum was first defined by Hasse by a formula of the type  $\tau(\chi) = W(\chi) \sqrt{N(\tilde{\chi})}$ , where  $W(\chi)$  is the Artin root number and the tilde means that one must

first choose a sign for the absolute norm of the conductor and then extract an appropriate square root. Note that  $\sqrt{N(\mathfrak{f}(\chi))}$  is the product of the usual  $\sqrt{N(\mathfrak{f}(\chi))}$  by a fourth root of unity. Following Fröhlich, we define this root of unity as an "infinite part" of the root number. Moreover, to be consistent with the preceding sections, we consider  $W(\bar{\chi})$  instead of  $W(\chi)$ .

Definition 7.1. For every infinite place  $v$  of  $K$ , let  $W_v(\chi) = i^{-n(\chi, v)}$ , where  $n(\chi, v)$  is the integer defined in §1. The infinite part of the root number is the complex number  $W_\infty(\chi) = \prod_{v \text{ infinite}} W_v(\chi)$ .

Definition 7.2. The Galois Gauss sum  $\tau(\chi)$  is the complex number defined by

$$\tau(\chi) = W(\bar{\chi}) \sqrt{N(\mathfrak{f}(\chi))} W_\infty(\chi)^{-1},$$

where  $W(\bar{\chi})$  is the Artin root number, and  $\sqrt{N(\mathfrak{f}(\chi))}$  is the positive square root of the positive generator of the absolute norm of the Artin conductor.

Note that  $\mathfrak{f}(\bar{\chi}) = \mathfrak{f}(\chi)$ , and that  $W_\infty(\bar{\chi}) = W_\infty(\chi)$  (For the latter equality, just remark that  $n(\chi, v) = n(\chi_v)$ , where  $\chi_v$  is the local character on the completion of  $K$  at  $v$

defined by  $\chi_v$ ; hence,  $\bar{\chi}_v = \chi_v$  and  $W_v(\bar{\chi}_v) = W_v(\chi)$  for every infinite place  $v$  of  $K$ ). Thus, the following equality holds:

$$W(\chi) = \frac{\tau(\bar{\chi}) W_\infty(\chi)}{\sqrt{N(f(\chi))}}.$$

Remark (Exercise)  $W(\chi) \tau(\chi) = \sqrt{N(f(\chi))} W_\infty(\chi)^{-1}$ . (Hint: prove the equality  $W_v(\chi)^2 = \det_{\chi_v}(-1)$  for any infinite place  $v$ ).

Proposition 7.1.  $\tau(\chi) = \prod_{p \text{ finite}} \tau(\chi_p),$

where  $\chi_p$  is the local character on the Galois group

$G_{K_p} = \text{Gal}(\bar{\mathbb{Q}}_p/K_p)$  of the completion of  $K$  at  $p$  ( $\bar{\mathbb{Q}}_p$  is a given algebraic closure of  $\mathbb{Q}_p$ , and  $p$  lies above  $p$ ).

Proof. The Artin root number  $W(\chi)$  is the product  $\prod_v W(\chi_v)$  where  $v$  runs through all places of  $K$  (see J. Tate, Durham).

$$\text{Now, } W_\infty(\chi) = \prod_{v \text{ infinite}} W_v(\chi) = \prod_{v \text{ infinite}} W(\chi_v).$$

$$\text{Hence, } W(\bar{\chi}) W_\infty(\chi)^{-1} = W(\bar{\chi}) W_\infty(\bar{\chi})^{-1} = \prod_{p \text{ finite}} W(\bar{\chi}_p).$$

Now, the positive rational number  $N(f(\chi))$  is also the product  $\prod_{p \text{ finite}} N(f(\chi_p))$ . Therefore

$$\tau(\chi) = \frac{W(\bar{\chi}) W_{\infty}(\bar{\chi})^{-1}}{\sqrt{N(\chi)}} = \prod_{p \text{ finite}} \frac{W(\bar{\chi}_p)}{\sqrt{N(\chi_p)}} = \prod_{p \text{ finite}} \tau(\chi_p).$$

We shall now use proposition 7.1. to derive global results from the local results of §5. and §6.

Theorem 7.2. (Fröhlich) For every  $\omega \in \Omega_{\mathbb{Q}}$ ,

$$\tau(\chi^{\omega^{-1}})^{\omega} = \tau(\chi) \det_{\chi}(\text{Ver}_{K/\mathbb{Q}}(\omega)) .$$

Proof. For every finite prime  $p$  of  $K$ ,  $(\chi_p)^{\omega^{-1}} = (\chi^{\omega^{-1}})_p$ ;

hence,

$$\frac{\tau(\chi^{\omega^{-1}})^{\omega}}{\tau(\chi)} = \prod_{p \text{ finite}} \frac{\tau(\chi_p^{\omega^{-1}})^{\omega}}{\tau(\chi_p)} = \prod_{p \text{ finite}} \det_{\chi_p}(\text{Ver}_{K_p/\mathbb{Q}_p} V_p(\omega))$$

with the notation of corollary 5.2.

The theorem we want to prove is now a consequence of the following lemma of class field theory.

Lemma 7.3. For any irreducible character of degree one  $\psi$  of  $\Omega_K$ ,

$$\psi(\text{Ver}_{K/\mathbb{Q}}(\omega)) = \prod_{p \text{ finite}} \psi_p(\text{Ver}_{K_p/\mathbb{Q}_p}(V_p(\omega))).$$

Proof of the lemma. When  $K = \mathbb{Q}$ , the formula we want to

prove is simply

$$\psi(\omega) = \prod_{p \text{ finite}} \psi_p(V_p(\omega)) \text{ for any } \omega \in \Omega_{\mathbb{Q}}^{\text{ab}}.$$

It is a consequence of the discussion of the reciprocity law over the rationals (see Artin-Tate's notes, chap. 6. §2). The general case is an easy consequence of the commutative diagram of §3.

Remark. Theorem 7.2. can be stated in terms of idèles. Define  $u : \Omega_{\mathbb{Q}} \rightarrow I_{\mathbb{Q}}$  by  $u_{\infty} = 1$  and  $u(\omega)_p = u_p(\omega)$  for every finite prime  $p$ . Then:

$$\tau(\chi^{\omega^{-1}})^{\omega} = \tau(\chi) \det_{\chi}(u(\omega)),$$

where  $\det_{\chi}(x)$  for an idèle  $x$  is simply the value of  $\det_{\chi}$  on the element  $s \in \Omega_K^{\text{ab}}$  which is the image of  $x$  under the Artin map.

The particular case of tame and real valued characters can be dealt with easily, as in the local case. We obtain the following theorem due to Fröhlich.

Theorem 7.4. Let  $K$  be a number field, and let  $\chi$  be a character of  $\Omega_K$ . Assume that  $\chi$  is tame and real valued. Then, the following results hold:

- (i) For every  $\omega \in \Omega_K$ ,  $W(\chi^{\omega}) = W(\chi)$

(ii)  $\tau(\chi) / \tau(\det_{\chi})$  is a rational number

(iii)  $W_{\infty}(\chi) / W_{\infty}(\det_{\chi}) = +1$  or  $-1$

(iv) if  $\chi$  is a character with trivial determinant,

then  $\tau(\chi)$  is a rational number whose sign is the product of the signs of  $W(\chi)$  and  $W_{\infty}(\chi)$ .

Proof As  $\chi$  factors through a tamely ramified extension, so does  $\det_{\chi}$ . By additivity,  $\tau(\chi) / \tau(\det_{\chi}) = \tau(\chi - \det_{\chi})$  and  $W_{\infty}(\chi) / W_{\infty}(\det_{\chi}) = W_{\infty}(\chi - \det_{\chi})$ . As  $\chi - \det_{\chi}$  has trivial determinant, it is enough to prove (ii) and (iii) for a character with trivial determinant.

Now, for every finite prime  $p$  of  $K$ ,  $\chi_p$  is a tame real valued character with trivial determinant. Hence, by propositions 6.1. and 6.2.,  $\tau(\chi_p)$  is rational. As  $\tau(\chi_p) = +1$  for almost all  $p$ ,  $\tau(\chi) = \prod_p \tau(\chi_p)$  is rational. We have thus proved (ii). Moreover,  $N(\mathfrak{f}(\chi)) = \prod_p N(\mathfrak{f}(\chi_p))$  is a square by proposition 6.2. As  $\chi$  is real valued,  $W(\chi) = +1$  or  $-1$ . Hence,  $W_{\infty}(\chi) = \frac{W(\chi) \sqrt{N(\mathfrak{f}(\chi))}}{\tau(\chi)}$  is a rational number. As it is a 4<sup>th</sup> root of unity,  $W_{\infty}(\chi) = +1$  or  $-1$ , and this proves the assertions (iii) and (iv).

We must now prove (i). We need the following lemma:

Lemma 7.5. Let  $\psi$  be a homomorphism of  $\Omega_K$  into  $\{-1, +1\}$ .  
Then  $W(\psi) = +1$ .

Proof of the lemma. We know that the Artin root number of a zeta function is  $+1$ . If  $\psi$  is trivial,  $L(s, \psi) = \zeta_K(s)$ , hence  $W(\psi) = +1$ . If  $\psi$  is not trivial, then  $\psi$  corresponds to a quadratic extension  $E/K$ , and  $L(s, \psi) = \zeta_E(s)/\zeta_K(s)$ . Thus,  $W(\psi) = W(\zeta_E)/W(\zeta_K) = +1$ .

Proof of (i). Let  $\omega \in \Omega_K$ . By the above lemma,  $W(\det_\chi) = W(\det_\omega) = +1$ . Hence,  $W(\chi^\omega) = W((\chi - \det_\chi)^\omega)$  and  $W(\chi) = W(\chi - \det_\chi)$ . We may therefore assume that  $\chi$  is a character with trivial determinant. We now use the formula

$$W(\chi) = \prod_v W(\chi_v)$$

where  $v$  runs through all places of  $K$ . By the results of

§6.,  $W(\chi_v^\omega) = W(\chi_v)$ . Hence,  $W(\chi^\omega) = \prod_v W(\chi_v^\omega) = \prod_v W(\chi_v) = W(\chi)$ , Q.E.D.

Remark. Without the assumption that  $\chi$  is tame conclusions (i), (ii) and (iv) of the theorem are no longer valid. See e.g. [7a] §9, or [7b] Theorem 19.



### §8. Global induction formulae

We give in this section induction formulae for the infinite part of the root number and the Galois Gauss sum. These formulae were originally used by Fröhlich to prove the results of §7. We give them for their own interest.

Definition. Let  $K$  be a number field. For any finite extension  $E$  of  $K$  and any place at infinity  $v$  of  $K$ , define

$$t(E/K, v) = 0 \text{ if } v \text{ is complex,}$$

$$t(E/K, v) = \text{the number of complex places of } E \\ \text{lying above } v \text{ if } v \text{ is real.}$$

$$\text{Put } t(E/K) = \sum_{v \text{ real}} t(E/K, v).$$

Theorem 8.1. Let  $E$  be finite normal extension of a number field  $K$  with Galois group  $G$ . Let  $H$  be a subgroup of  $G$  corresponding to a field  $F$ . Let  $\chi$  be a character of  $H$ , and let  $\chi^*$  be the character of  $G$  induced by  $\chi$ .

(i) For every place  $v$  of  $K$ ,

$$n(\chi^*, v) = \sum_{\substack{w|v \\ w \text{ in } F}} n(\chi, w) + \chi(1) t(F/K, v)$$

$$(ii) \quad W_{\infty}(\chi^*) = W_{\infty}(\chi) i^{-\chi(1) t(F/K)}$$

$$(iii) \quad \tau(\chi^*) = \tau(\chi) \cdot [N(D(F/K))]^{\frac{1}{2}} \cdot i^{t(F/K)} \chi(1),$$

where  $N(D(F/K))$  is the absolute norm of the discriminant of  $F$  over  $K$ .

Proof. (ii) is an obvious consequence of (i), and (iii) is easily deduced from (ii): write

$$\frac{\tau(\chi^*)}{\tau(\chi)} = \frac{W(\chi^*)}{W(\chi)} \left[ \frac{N(\delta(\chi^*))}{N(\delta(\chi))} \right]^{\frac{1}{2}} \left[ \frac{W_\infty(\chi^*)}{W_\infty(\chi)} \right]^{-1}.$$

Then,  $W(\chi^*) = W(\chi)$ ,  $\frac{W_\infty(\chi^*)}{W_\infty(\chi)} = i^{-t(F/K)\chi(1)}$  by (ii) and the

equality  $\frac{N(\delta(\chi^*))}{N(\delta(\chi))} = N(D(F/K))^{\chi(1)}$  is an easy consequence of the calculation of the conductor of an induced character.

We are now left with the proof of (i). If  $\chi$  is of degree zero, the formula we want to prove is:

$$n(\chi^*, v) = \sum_{\substack{w|v \\ w \text{ in } F}} n(\chi, w).$$

But  $n(\chi, w) = n(\chi_w)$  and  $n(\chi^*, v) = n((\chi^*)_v)$ . Thus, the desired formula is a consequence of the formula which gives the restriction of an induced representation (see e.g. Serre, Représentations linéaires des groupes finis, chap. 7, prop. 22). It is thus enough to prove (i) when  $\chi$  is the unit character.

Since  $n(\chi, w) = 0$ , formula (i) can be written

$$n(\chi^*, v) = t(F/K, v).$$

The equality is obvious when  $v$  is complex. Assume  $v$  is real, and let  $\sigma$  be the "Frobenius" of a place  $w$  above  $v$  in  $E$ . Then,  $n(\chi^*, v) = \frac{1}{2} (\chi^*(1) - \chi^*(\sigma))$ . Now  $\chi^*(1) = [F:K]$ , and  $\chi^*(\sigma) = \sum_{t \in G/H} \chi(t\sigma t^{-1})$ . But  $\chi(t\sigma t^{-1}) = 1$  if  $tw$  lies above a real place of  $F$  (for  $t\sigma t^{-1} \in H$ ) and  $\chi(t\sigma t^{-1}) = 0$  otherwise. Hence,  $\chi^*(1) - \chi^*(\sigma)$  is the number of elements of  $G \bmod H$  such that  $tw$  lies above a complex place of  $F$ , and this number is precisely  $2t(F/K, v)$ , Q.E.D.

### III. ORTHOGONAL AND SYMPLECTIC REPRESENTATIONS

#### §1. Description of real valued characters

Let  $G$  be a finite group, and let  $K$  be a subfield of the field  $\mathbb{C}$  of complex numbers. Given a finite dimensional  $K$ -vector space  $V$  and a representation  $\rho : G \rightarrow \text{Gl}(V)$ , we define a complex representation  $\rho' : G \rightarrow \text{Gl}(\mathbb{C} \otimes_K V)$  by  $\rho'_s(1 \otimes x) = 1 \otimes \rho_s(x)$ . We call such a complex representation a  $K$ -representation.

Consideration of direct sums and tensor products of  $K$ -representations shows that the set  $R_G^K$  of characters of  $K$ -representations of  $G$  is a subring of the ring  $R_G$  of characters of  $G$ . Clearly, a character  $\chi \in R_G^K$  has its values in  $K$ . The converse however is not true. We denote by  $\bar{R}_G^K$  the subring of  $R_G$  which consists of characters of  $G$  with values in  $K$ .

We are interested in the case when  $K = \mathbb{R}$ , the field of real numbers. The rings  $R_G^{\mathbb{R}}$  and  $\bar{R}_G^{\mathbb{R}}$  are then related to geometrical invariants.

We denote by  $R_G^b$  the set of characters of  $R_G$  which are

the difference of 2 characters of representations preserving a non degenerate bilinear form. We shall call a non-degenerate bilinear form orthogonal (resp. symplectic) if it is symmetric (resp. skew-symmetric). We define the subset  $R_G^O$  (resp.  $R_G^S$ ) of  $R_G^b$  to be the set of characters  $\chi \in \mathbb{R}_G$  which are differences of 2 characters of representations preserving an orthogonal (resp. symplectic) form. The virtual characters in  $R_G^O$  will be called orthogonal, those in  $R_G^S$  symplectic. The sets  $R_G^b$ ,  $R_G^O$  and  $R_G^S$  are subgroups of  $R_G$ . Moreover, consideration of tensor products shows immediately that  $R_G^b$  and  $R_G^O$  are subrings of  $R_G$ , whereas  $R_G^S$  is a module over  $R_G^O$ . Note that every symplectic character has even degree and trivial determinant.

Let  $T : R_G \rightarrow R_G$  be the map  $\chi \mapsto \chi + \bar{\chi}$ .

- Theorem 1.1.      (i)       $R_G^b = \bar{R}_G^{\mathbb{R}}$
- (ii)       $R_G^O = R_G^{\mathbb{R}}$
- (iii)      $R_G^b = R_G^O + R_G^S$
- (iv)      $R_G^O \cap R_G^S = \text{Im } T$ .

For a proof, see e.g. Serre, [12], §13.

We can now define three (mutually exclusive) types of irreducible real valued characters.

Type 1.  $\chi = \phi + \bar{\phi}$ , where  $\phi \in R_G$  is absolutely irreducible and takes at least one non real value.

Type 2.  $\chi$  is an absolutely irreducible character and is orthogonal.

Type 3.  $\chi$  is an absolutely irreducible character and is symplectic.

These characters are irreducible real valued characters, and make a basis of  $\bar{R}_G^{\mathbb{R}}$ , from which bases of  $R_G^O$  and  $R_G^S$  are easily deduced.

Irreducible real valued characters are in one-to-one correspondence with the simple algebras which occur in a decomposition of the semi-simple algebra  $\mathbb{R}(G)$ . For  $\chi$  of type (1), the centre of the corresponding algebra is  $\mathbb{R}(\phi) = \mathbb{C}$ . Hence, the simple algebra corresponding to  $\chi$  is isomorphic to  $M_n(\mathbb{C})$  with  $n = \chi(1)$ . For  $\chi$  of type (2), the corresponding simple algebra is obviously isomorphic to  $M_n(\mathbb{R})$ , with  $n = \chi(1)$ . Therefore, a character of type (3) corresponds to a simple algebra isomorphic to  $M_n(\mathbb{H})$ , where  $\mathbb{H}$  denotes the skew-field of Hamilton quaternions and  $2n = \chi(1)$ . This last isomorphism can be described as

follows: start with an absolutely irreducible symplectic representation  $\rho : G \rightarrow \text{Gl}(V)$ , where  $V$  is a complex vector space of dimension, say,  $2n$ . Then  $\rho$  defines a representation  $\rho_{\mathbb{R}} : G \rightarrow \text{Gl}(V_{\mathbb{R}})$  where  $V_{\mathbb{R}}$  is the vector space  $V$  viewed as a real vector space (hence,  $\dim V_{\mathbb{R}} = 4n$ ). Let  $D$  be the ring of those endomorphisms of  $V_{\mathbb{R}}$  which commute with  $\rho_s$  for all  $s \in G$ . The ring  $D$ , which is a skew-field by Schur's lemma, is actually isomorphic to  $\mathbb{H}$ , and  $V_{\mathbb{R}}$  can therefore be given a structure of  $\mathbb{H}$ -vector space of dimension  $n$ , say  $V_{\mathbb{H}}$ . Now the simple algebra corresponding to  $\rho$  is the ring  $\text{End}_{\mathbb{H}}(V_{\mathbb{H}})$ , isomorphic to  $M_n(\mathbb{H})$ .

## §2. Induction theorems

a) The Brauer-Witt theorem Given a subfield  $K$  of  $\mathbb{C}$  and a prime number  $p$ , one can define  $\Gamma_K$ - $p$ -elementary groups, which are semi-direct products of a normal cyclic subgroup  $C$  of order prime to  $p$  by a  $p$ -group  $p$  (for a definition, see e.g. [12], §12). For  $K = \mathbb{C}$ , the semi-direct product is actually a direct product, and  $\Gamma_K$ - $p$ -elementary groups are the "usual" elementary groups. For  $K = \mathbb{R}$ , the following condition must hold : for every  $y \in P$ , there exist  $t \in \{-1, +1\}$ , such that, for every  $x \in C$ ,  $yx y^{-1} = x^t$ .



A group is called  $\Gamma_K$ -elementary if it is  $\Gamma_K$ - $p$ -elementary for some  $p$ .

Theorem 2.1. (Brauer-Witt theorem) Every  $K$ -character of a finite group  $G$  is a  $\mathbb{Z}$ -linear combination of characters of the form  $\text{Ind}_H^G(\chi)$ , where  $H$  is a  $\Gamma_K$ -elementary subgroup of  $G$  and  $\chi$  is a  $K$ -character of  $H$ .

Remark. A  $\Gamma_K$ -elementary group is supersolvable (see the definition below). Hence, every irreducible character of  $H$  is induced by a character of degree one of some subgroup. Taking  $K = \mathbb{C}$ , one has the "usual" Brauer theorem used in chapter 1.

b) The Borel-Serre theorem. Call a group  $G$  supersolvable if there exists a sequence  $\{e\} = G_0 \subset G_1 \subset \dots \subset G_{k-1} \subset G_k = G$  of normal subgroups of  $G$  such that  $G_i/G_{i-1}$  is cyclic.

The following theorem was proved by Borel and Serre in 1953 ([2]).

Theorem 2.2. (Borel-Serre theorem) Let  $L$  be a compact Lie group, and let  $G$  be a supersolvable subgroup of  $L$ .

Then,  $G$  is contained in the normalizer  $N$  of a maximal torus  $T$  of  $L$ .

We make a few comments on this theorem.

- 1) The inclusion  $G \subset N$  simply means that, for every  $s \in G$  and every  $t \in T$ ,  $sts^{-1} \in T$ .
- 2) Two maximal tori of  $L$  are conjugate.

### §3. Induction theorems for orthogonal characters

Definition The dihedral group  $D_{2n}$  of order  $2n$  is the group on 2 generators  $\sigma$  and  $\tau$  with relations  $\sigma^n = \tau^2 = 1$ ,  $\tau\sigma\tau^{-1} = \sigma^{-1}$ . Note that it is the semidirect product of its subgroups generated by  $\sigma$  and by  $\tau$ .

All the characters of  $D_{2n}$  are orthogonal. There are 2 (resp. 4) irreducible characters of degree one of  $D_{2n}$  if  $n$  is odd (resp. even). The remaining irreducible characters of  $D_{2n}$  are of degree 2.

Definition Let  $G$  be a finite group. An character  $\chi$  of  $G$  is called a dihedral character if  $\chi$  factors through a dihedral quotient of  $G$  and is irreducible of degree 2.

The following theorem is extracted from Serre's paper

on Artin-conductors ([13] ; see also D. Quillen, [10], lemma 2.4).

Theorem 3.1. (Serre) Let  $G$  be a finite group, and let  $\chi$  be an orthogonal character of  $G$ . Then,  $\chi$  is a  $\mathbb{Z}$ -linear combination of characters of the form  $\text{Ind}_H^G(\phi)$  where  $H$  is a subgroup of  $G$  and  $\phi$  satisfies one of the 3 following conditions:

- (i)  $\phi$  is a homomorphism of  $H$  into  $\{-1, +1\}$
- (ii)  $\phi = \psi + \bar{\psi}$ , where  $\psi$  is an irreducible character of degree one of  $H$
- (iii)  $\phi$  is a dihedral character of  $H$ .

Proof. By theorem 2.1, we may assume that  $G$  is a  $\Gamma_{\mathbb{R}}$ -elementary group and that  $\chi$  is an irreducible orthogonal character. Since every  $\Gamma_{\mathbb{R}}$ -elementary group is supersolvable, theorem 3.1 is a consequence of the following more precise result for supersolvable groups.

Theorem 3.2. Let  $G$  be a finite supersolvable group and let  $\chi$  be an irreducible orthogonal character of  $G$ . Then, one of the following conditions holds:

- (i)  $\chi$  is a homomorphism of  $G$  into  $\{-1, +1\}$
- (ii)  $\chi = \psi + \bar{\psi}$ , where  $\psi$  is induced by an irreducible character of degree 1 of some subgroup of  $G$
- (iii)  $\chi$  is induced by a dihedral character of some subgroup of  $G$ .

Proof. Let  $n = \chi(1)$ . The character  $\chi$  is the character of a representation  $\rho : G \rightarrow \text{Gl}(V)$  where  $V$  is a real vector space of dimension  $n$ . The group  $\rho(G)$  is contained in the orthogonal group  $O(V)$  of some positive definite bilinear form on  $V$ . By theorem 3.2,  $\rho(G)$  is contained in the normalizer of a maximal torus  $T$  of  $O(V)$ . Let  $m = [\frac{n}{2}]$ . There exists a subspace  $W$  of  $V$  of dimension  $2m$  such that the matrix of  $T$  in a suitable basis  $e_1, \dots, e_{2m}$  of  $W$  is of the form

$$\begin{pmatrix} \boxed{SO_2} & & & & 0 \\ & \boxed{SO_2} & & & \\ & & \ddots & & \\ & & & \boxed{SO_2} & \\ 0 & & & & \end{pmatrix}$$

Let  $w_i$  ( $1 \leq i \leq m$ ) be the subspace of  $W$  spanned by the vectors  $e_{2i-1}, e_{2i}$ . Now, there are two possibilities:

a) n is odd. Since  $W$  is invariant under the action of  $G$ ,  $V$  contains an invariant subspace  $W'$  of dimension 1. Since  $\rho$  is irreducible,  $W = (0)$  and  $V = W'$ . The character  $\chi$  is then of type (i).

b) n is even. Let  $H$  be the subgroup of those elements  $s \in G$  such that  $\rho_s(W_1) \subset W_1$ . Since  $\rho(G)$  is contained in the normalizer of  $T$ ,  $\rho(G)$  permutes the subspaces  $W_i$ . Since  $\rho$  is irreducible, this permutation is transitive. This means that  $\rho$  is induced by the representation  $\rho_1 : H \rightarrow \text{Gl}(W_1)$  deduced from  $\rho$  by restriction to  $H$ . But  $\rho_1$  is a real representation. Therefore,  $\rho_1(H)$  is isomorphic to a subgroup of  $O_2(\mathbb{R})$  and  $\chi$  is of type (iii) or (ii) according to whether  $\rho_1$  is absolutely irreducible or not.

We shall now give a corollary of theorem 3.1. due to Deligne ([4] ; Deligne's paper also contains a purely group theoretic proof of theorem 3.1). We must first extend slightly the definition of a dihedral character : we consider that a character lifted from a character  $\chi'$  of a quotient of  $G$  isomorphic to  $D_4$  is a dihedral character if  $\chi'$  is the sum of 2 distinct irreducible characters of degree 1.

Definition Let  $G$  be a finite group. Let  $\chi$  be a dihedral character of  $G$  lifted from a character  $\chi'$  of a dihedral quotient  $G'$  of  $G$ . Then,  $\chi' = \text{Ind}_{H'}^{G'}(\phi')$ , where  $H'$  is a cyclic subgroup of  $G'$  of index 2 and  $\phi'$  is an irreducible character of degree 1. We call  $r_\chi$  the character of  $G$  lifted from  $\text{Ind}_{H'}^{G'}(\phi' - 1)$ .

Note that  $r_\chi$  has degree 0 and trivial determinant.

Theorem 3.3. (Deligne) Let  $G$  be a finite group. Every orthogonal character of  $G$  of degree 0 and trivial determinant is a  $\mathbb{Z}$ -linear combination of characters of the form  $\text{Ind}_H^G(\phi)$  where  $\phi$  is either a character  $r_\chi$  or a sum  $\psi + \bar{\psi}$  with  $\psi(1) = 0$ .

Proof. Let  $\chi$  be a character of  $G$  of degree 0 and trivial determinant. By Brauer-Witt's theorem, the unit character of  $G$  can be written as a sum  $1 = \sum_H n_H \text{Ind}_H^G(\phi_H)$  where  $H$  ranges over the  $\Gamma_{\mathbb{R}}$ -elementary subgroups of  $G$  and  $\phi_H$  is an orthogonal character of  $H$ . Now,  $\chi = \chi \cdot 1 = \sum_H n_H \text{Ind}_H^G(\text{Res}_G^H(\chi) \cdot \phi)$ . Since  $\text{Res}_G^H(\chi)$  has degree 0 and trivial determinant, so does  $\text{Res}_G^H(\chi) \cdot \phi$ . We may therefore assume that  $G$  is a  $\Gamma_{\mathbb{R}}$ -elementary group.

Let  $A$  be the subgroup of  $R_G^0$  generated by the characters



of the form of theorem 3.3. With the notation of theorem 3.2, let  $B$  (resp.  $C$ ,  $D$ ) be the subgroup of  $R_G^O$  generated by characters of type (i) (resp. (ii), (iii)).

Lemma 3.4. If  $G$  is  $\Gamma_{\mathbb{R}}$ -elementary, then  $R_G^O = A+B$ .

Proof of lemma 3.4. It is enough to prove that every irreducible orthogonal character  $\chi$  belongs to  $A+B$ . If  $\chi(1) = 1$ , there is nothing to prove. We can therefore prove the lemma by induction on  $\chi(1)$ . If  $\chi \in C$ , say  $\chi = \text{Ind}_H^G(\psi + \bar{\psi})$  with  $\psi(1) = 1$ , write

$$\chi = \text{Ind}_H^G [(\psi(1) - 1) + \overline{(\psi(1))} - 1] + 2 \cdot 1^*.$$

Since  $1^*(1) < \chi(1)$ , the induction process works.

If  $\chi \in D$ , say  $\chi = \text{Ind}_H^G(\Phi)$  where  $\Phi$  is a dihedral character, write  $\Phi = r_{\Phi} + (\Phi - r_{\Phi})$ . Since  $\Phi - r_{\Phi}$  contains the unit character, the induction process works.

Proof of theorem 3.3. By lemma 3.4., it is enough to show that any character  $\chi \in B$  with degree 0 and trivial determinant belongs to  $A$ . Since  $\chi(1) = 0$ , we may write  $\chi$  as a sum  $\chi = \sum_{i=1}^n \epsilon_i (\Phi_i - 1)$ , where the  $\Phi_i$ 's are homomorphisms of  $G$  onto  $\{-1, +1\}$  and  $\epsilon_i = +1$  or  $-1$ . Since



$2(\phi_i - 1) = \overline{(\phi_i - 1)} + (\phi_i - 1) \in A$ , we may assume that  $\varepsilon_1 = \varepsilon_2 = +1$  and  $\varepsilon_i = -1$  for  $i \geq 3$ . The result we want to prove is obvious for  $n \leq 2$ . For  $n = 3$ ,  $\chi = \phi_1 + \phi_2 - \phi_3 - 1$ . Since  $\det_\chi$  is trivial,  $\phi_3 = \phi_1 \phi_2$ . If  $\phi_1 = \phi_2$ , then  $\chi = 2(\phi_1 - 1) \in A$ . If  $\phi_1 \neq \phi_2$ , let  $H = \text{Ker } \phi_1 \cap \text{Ker } \phi_2$ . Then,  $G/H$  is isomorphic to  $D_4$ , and  $\psi = r_{\phi_1 + \phi_2} \in A$ . For  $n > 3$ , the theorem is obvious by induction on  $n$ : just write  $\chi = (\phi_1 + \phi_2 - \phi_1 \phi_2 - 1) + (\phi_1 \phi_2 - 1) - \sum_{i=3}^n (\phi_i - 1)$ , and remark that  $\chi$  is congruent mod  $A$  to  $(\phi_1 \phi_2 - 1) + (\phi_3 - 1) - \sum_{i=4}^n (\phi_i - 1)$ .

#### §4. Some arithmetic properties of orthogonal characters

We first prove a theorem of Serre on conductors of real representations.

Theorem 4.1. Let  $K$  be a number field or a finite extension of a  $p$ -adic field. Let  $E$  be a finite normal extension of  $K$  with Galois group  $G$ , and let  $\chi$  be a real-valued character of  $G$ . Assume that one of the following conditions holds:

- (i)  $E/K$  is tamely ramified
- (ii)  $\chi$  is an orthogonal character

Then,  $f(\chi)/f(\det_\chi)$  is the square of an ideal.

Corollary 4.2. Under the assumptions of the theorem, the class of the ideal  $\delta(\chi)$  is a square.

Proof. There is nothing to prove if  $\det_\chi$  is trivial. If  $\det_\chi$  is not trivial, then it is the character of a quadratic extension  $F/K$ , and  $\delta(\det_\chi)$  is the discriminant of the extension  $F/K$ . Hence, its class is a square.

Corollary 4.3. Let  $K$  be a finite extension of a  $p$ -adic field. Assume that  $\chi$  has trivial determinant. Then, under the assumption of the theorem, the local root number  $W(\chi)$  depends only on the conjugacy class of  $\chi$  (i.e.,  $: W(\chi^\omega) = W(\chi)$  for any  $\omega \in \Omega_{\mathbb{Q}}$ ).

Proof. This is an obvious consequence of chap. II, prop. 6.1.

Proof of theorem 4.1. We first remark that  $\delta(\chi)/\delta(\det_\chi) = \delta(\chi - \det_\chi)$ . We may therefore assume that  $\chi$  is a character with trivial determinant; we must then prove that  $\delta(\chi)$  is a square, or, with the notation of chap. II, §1, that  $n(\chi, p)$  is an even integer for every finite prime  $p$  of  $K$ .

Since  $n(\chi, p) = n(\chi_p)$ , it is enough to prove the theorem when  $K$  is a finite extension of a  $p$ -adic field.

There is a field  $E'$ ,  $K \subset E' \subset E$ , such that  $E'/K$  is unramified and  $E/E'$  is totally ramified. If  $H$  is the subgroup of  $G$  corresponding to  $E'$ , then the conductors of  $\chi$  and  $\chi|_H$  have the same valuation. Hence, we may assume that  $E/K$  is totally ramified.

Now, the case of a tame extension has already been dealt with (chap. II. §6). We therefore assume that  $\chi$  is an orthogonal character. Since  $f(\chi) = f(\chi - \chi(1).1)$ , we may assume that  $\chi$  is a character of degree 0. By theorem 3.3., we are reduced to the case when  $\chi = \phi + \bar{\phi}$  or  $\chi = r_\phi$ . Since  $f(\chi + \bar{\chi}) = f(\chi)^2$ , we need only consider the case when  $E/K$  is a totally ramified dihedral extension and  $\chi$  is a character of the form  $r_\phi$ .

The character  $r_\phi$  is induced by a character of the form  $(\phi - 1)$  of a cyclic subgroup  $H$  of  $G$  of index 2, where  $\phi$  is irreducible of degree 1. Denote by  $F$  the fixed field of  $H$ . Using the Artin map, we can view  $\phi$  as a character on  $F^*$ . We know that the conductor of  $\phi$  is the least integer  $t$  such that  $\phi$  is trivial on  $U_F^t$ , and we must prove that this integer is even. The following proof has been given to me

by Serre. (cf. Exercise 7).

Any easy calculation shows that the transfer from  $G^{\text{ab}}$  to  $H$  is trivial. Hence,  $\phi$  has a trivial restriction to  $K^*$ . On the other hand, since  $F/K$  is totally ramified, the inclusion  $i : K^* \rightarrow F^*$  induces for every  $n$  an isomorphism  $i_n : U_K^n / U_K^{n+1} \rightarrow U_F^{2n} / U_F^{2n+1}$ . Therefore, if  $\phi$  is trivial on  $U_F^{2n+1}$ , then  $\phi$  is trivial on  $U_F^{2n}$ . Hence, the least integer  $t$  such that  $\phi$  is trivial on  $U_F^t$  is even, Q.E.D.

Remark 4.1. The conclusion of theorem 4.1. need not hold if the real valued character  $\chi$  is not orthogonal; for example, see [13], or [7a] (Theorem 6).

Remark 4.2. Serre actually proved a more general theorem, namely : let  $A$  be a Dedekind domain with quotient field  $K$ ; let  $E$  be finite normal extension of  $K$  with Galois group  $G$ , and let  $\chi$  be a character of  $G$ . Assume that all the residue extensions of  $E/K$  are separable. Then, under the assumptions of theorem 4.1.,  $\delta(\chi) / \delta(\det_\chi)$  is a square. The proof is also by reduction to the dihedral case. (cf. Exercise 8).

Remark 4.3. The corresponding global statement to corollary 4.3. is true. By a theorem of Fröhlich and Queyrut (see Tate (Durham)),  $W(\chi) = +1$ . The equality  $W(\chi^\omega) = W(\chi)$  for every  $\omega \in \Omega_{\mathbb{Q}}$  is therefore trivial. Note that the original proof of the theorem of Fröhlich and Queyrut used a reduction to the case of a dihedral extension; the equality  $W(\chi) = +1$  was then proved by direct calculation.

### §5. Induction theorems for symplectic characters.

Definition. The quaternion group  $H_{4n}$  of order  $4n$  is the group on 2 generators  $\sigma$  and  $\tau$  with relations :  $\sigma^n = \tau^2$ ,  $\tau^4 = 1$ ,  $\tau\sigma\tau^{-1} = \sigma^{-1}$ ; it contains a unique element of order 2, namely  $\tau^2$ ;  $H_4$  is cyclic; for  $n > 1$ ,  $\{1, \tau^2\}$  is the centre of  $H_{4n}$ , and  $H_{4n}/\{1, \tau^2\}$  is the dihedral group  $D_{2n}$  of order  $2n$ . Note that  $H_{4n}$  is the non-trivial extension of the group  $C_2$  of order 2 by the cyclic subgroup generated by  $\sigma$ , the action of the generator of  $C_2$  being given by  $\sigma \mapsto \sigma^{-1}$ .

The group  $H_{4n}$  has 4 characters of degree 1. The other irreducible characters are real-valued characters of degree 2. Those which factor through a dihedral quotient are orthogonal, and those which do not are symplectic.

Definition Let  $G$  be a finite group. A quaternion character of  $G$  is an absolutely irreducible character of degree 2 of  $G$  which is lifted from a symplectic character of a quaternion quotient of  $G$ .

Theorem 5.1. Let  $G$  be a finite group and let  $\chi$  be a symplectic character of  $G$ . Then,  $\chi$  is a  $\mathbb{Z}$ -linear combination of characters of the form  $\text{Ind}_H^G(\phi)$  for some subgroup  $H$  of  $G$ , where:

- (i) either  $\phi = \psi + \bar{\psi}$ , where  $\psi$  is an irreducible character of degree 1 of  $H$ ,
- (ii) or  $\phi$  is a quaternion character of  $H$ .

Proof. Write for the unit character of  $G$  a decomposition  $1 = \sum_H n_H \text{Ind}_G^G(\chi_H)$  where  $H$  ranges over the  $\Gamma_{\mathbb{R}}$ -elementary subgroups of  $G$ ,  $n_H \in \mathbb{Z}$  and  $\chi_H$  is an orthogonal character. Then,

$$\chi = \chi \cdot 1 = \sum_H n_H \text{Ind}_H^G(\text{Res}_G^H(\chi) \cdot \chi_H).$$

Since  $R_G^S$  is a module over  $R_G^O$ ,  $\text{Res}_G^H(\chi) \cdot \chi_H$  is a symplectic character. Since a  $\Gamma_{\mathbb{R}}$ -elementary group is supersolvable, theorem 5.1. is a consequence of the following more precise result for supersolvable groups :



Theorem 5.2. Let  $G$  be a finite supersolvable group, and let  $\chi$  be an irreducible symplectic character of  $G$ .

Then one of the following conditions holds :

- (i)  $\chi = \Phi + \bar{\Phi}$ , where  $\Phi$  is induced by an irreducible character of degree one of some subgroup of  $G$ ;
- (ii)  $\chi$  is induced by a quaternion character of some subgroup of  $G$ .

Proof. Let  $\rho_{\mathbb{C}}$  be a complex representation with character  $\chi$ . If  $\chi$  is absolutely irreducible, we know from §1 that  $\rho_{\mathbb{C}}$  comes from a quaternion representation  $\rho : G \rightarrow V$  where  $V$  is a (say, left) vector space over the field  $\mathbb{H}$  of Hamilton quaternions. The same is true if  $\chi$  not absolutely irreducible. In both cases, the representation  $\rho$  is irreducible as a quaternion representation.

Let  $B$  be a quaternion-hermitian form on  $V$  invariant under  $G$ , and let  $L$  be the group of automorphisms of  $V$  which preserve  $B$ . Then,  $L$  is a compact Lie group, and  $\rho(G)$  is contained in the normalizer of a maximal torus  $T$  of  $L$ .

Now, consider in  $GL_n(\mathbb{H})$  the diagonal matrices



$$\begin{pmatrix} q_1 & & 0 \\ & \ddots & \\ 0 & & q_n \end{pmatrix}$$

with  $|q_i| = 1$ , where  $|q|$  is the norm of the quaternion  $q$ .

These matrices form a compact subgroup. Take for each index  $i$  a subgroup  $S_i$  of  $\mathbb{H}^*$  isomorphic to the circle. Then, it can be proved that the subgroup

$$\begin{pmatrix} S_1 & & 0 \\ & \ddots & \\ 0 & & S_n \end{pmatrix}$$

of  $GL_n(\mathbb{H})$  is a maximal torus, and every maximal torus of  $GL(V)$  is obtained by this construction after having chosen a suitable basis  $e_1, \dots, e_n$  of  $V$ , since two maximal tori are conjugate.

Going back to the proof of theorem 5.2, we can choose a basis  $e_1, \dots, e_n$  of  $V$  and subgroups  $S_1, \dots, S_n$  of  $\mathbb{H}^*$  such that

$$T = \begin{pmatrix} S_1 & & 0 \\ & \ddots & \\ 0 & & S_n \end{pmatrix} .$$

Let  $V_i$  ( $1 \leq i \leq n$ ) be the quaternion line  $\mathbb{H}e_i$ , and let  $H$  be the group of those  $s \in G$  such that  $\rho_s(V_1) \subset V_1$ . Since  $\rho(G)$  is contained in the normalizer of  $T$ ,  $\rho(G)$  permutes the  $V_i$ 's. Since  $\rho$  is irreducible, the permutation is transitive. Hence  $\rho$  is induced by  $\rho_1$ , the representation of  $H$  in  $Gl(V_1)$  obtained by restriction of  $\rho$  to  $H$ . Now,  $\rho_1(H)$  is a finite subgroup of  $\mathbb{H}^*$ , and the complete list of the finite subgroups of  $\mathbb{H}^*$  is known : if  $K$  is a non cyclic subgroup of  $\mathbb{H}^*$ ,  $K$  contains the elements  $\{-1, +1\}$  of  $\mathbb{H}^*$ , and  $K/\{-1, +1\}$  is isomorphic to a finite subgroup of  $SO_3(\mathbb{R})$ , hence is cyclic, dihedral or isomorphic to one of the three groups  $A_4$ ,  $D_4$ ,  $A_5$ . Therefore,  $K$  itself is cyclic, quaternion or isomorphic to one of the three "binary polyhedral groups"  $\tilde{A}_4$ ,  $\tilde{S}_4$ ,  $\tilde{A}_5$ . But the last three groups are not supersolvable, since  $A_4$ ,  $S_4$ ,  $A_5$  are not. Hence,  $\rho_1(H)$  is cyclic or quaternion, and  $\rho$  is of type (i) if  $\rho_1(H)$  is cyclic, of type (ii) otherwise. (Here is alternative proof :  $\rho_1(H)$  is contained in the normalizer  $N_1$  of  $S_1$ , and it is easy to find the structure of  $N_1$  :  $N_1 = \langle S_1, n \rangle$ , with  $nsn^{-1} = s^{-1}$  for every  $s \in S_1$  and  $n^2 = -1$ . Hence, either  $\rho_1(H)$  is contained in  $S_1$  and  $\rho_1(H)$  is cyclic, or  $\rho_1(H)$  is not contained in  $S_1$  and  $\rho_1(H)$

is quaternion.)

Remark. The conclusion of theorem 2.2 holds without the assumption that  $L$  should be compact. Hence, one can apply this theorem to the "usual" symplectic group  $Sp_{2n}(\mathbb{C})$  to obtain a proof of theorem 5.2. Nevertheless, quaternions are more suitable to study symplectic representations. Note that the unitary group associated to a quaternion-hermitian form is often called "the symplectic group" in the theory of Lie groups.

#### REFERENCES (II and III)

1. E. Artin and J. Tate, Class Field Theory, Princeton (1952).
2. A. Borel et J.-P. Serre. Sur certains sous-groupes des groupes de Lie compacts. Comm. Math. Helv., 27 (1953), 128-139.
3. J.W.S. Cassels and A. Fröhlich. Algebraic Number Theory. London and New York, Academic Press, 1967.
4. P. Deligne. Les constantes locales de l'équation fonctionnelle de la fonctions  $L$  d'Artin d'une représentation orthogonale (à paraître).
5. A. Fröhlich. Artin Root Numbers and Normal Integral Bases for Quaternion Fields., Invent. Math., 17, 2 (1972), 143-166.
6. A. Fröhlich. Resolvent and Trace Form. Math. Proc. Camb. Phil. Soc., 78 (1975), 185-210.

7. A. Fröhlich. Arithmetic and Galois Module Structure. To appear in Crelle.
- 7a. A. Fröhlich, Artin Root Numbers, Conductors and Representations for generalized Quaternion groups. Proc. London Math. Soc., 28 (1974) 402-438.
- 7b. A. Fröhlich, Galois module structure, Durham Symposium.
8. H. Hasse. Artinsche Führer, Artinsche L-Funktionen und Gaussssche Summen über endlich-algebraischen Zahlkörper., Universidad Salamanca (1954).
9. J. Martinet. Modules sur l'algèbre du groupe quaternionien., Ann. Sci. E.N.S., 4 (1971), 399-408.
10. D. Quillen. The Adams conjecture, Topology, 10 (1971), 67-80.
11. J.-P. Serre. Corps Locaux (deuxième édition) Paris, Hermann, 1968.
12. J.-P. Serre. Représentations linéaires des groupes finis, (deuxième édition). Paris, Hermann, 1971.
13. J.-P. Serre. Conducteurs d'Artin des caractères réels, Invent. Math. 14, 3 (1971), 173-183.
14. J. Tate, Local Constants, Durham Symposium.

## IV. EXERCISES (Prepared jointly with J.-P. Serre)

Exercise 1 (Dedekind) : Non abelian cubic fields.

Express the zeta function of a "pure" cubic field  $K = \mathbb{Q}(\sqrt[3]{\alpha})$  in terms of abelian L-functions of  $\mathbb{Q}(\sqrt[3]{1})$ . Generalize to any non abelian cubic field of discriminant  $D$  replacing  $\mathbb{Q}(\sqrt[3]{1})$  by  $\mathbb{Q}(\sqrt[3]{D})$ .

Exercise 2 : Artin conductors.

In this exercise,  $A$  is a Dedekind domain with quotient field  $K$ , and  $E$  is a finite normal extension of  $K$  with separable residue extensions. We consider representations  $\rho, \rho_1, \rho_2$  of  $G = \text{Gal}(E/K)$  into the linear groups of complex vector spaces  $V, V_1, V_2$  of respective dimensions  $n, n_1, n_2$ . Let  $N = [E : K]$ . Discriminants and conductors are relative to  $A$  (cf. II. §1).

a) Prove that  $f(\det_\rho)$  divides  $f(\rho)$ . (Hint: view  $\det_\rho$  as a representation of  $G$  into  $\text{Gl}(\wedge^n V)$ ).

b) Prove that if  $\rho$  is faithful, then the primes of  $K$  which divide  $f(\rho)$  are exactly those which divide the

discriminant  $D(E/K)$ . More precisely:

$b_1)$  If  $\rho$  is irreducible, then  $f(\rho)^n$  divides  $D(E/K)$ .

$b_2)$   $D(E/K)$  divides  $f(\rho)^{N-1}$ .

$b_3)$  If  $\det_\rho$  is trivial, then  $D(E/K)^2$  divides  $f(\rho)^{N-1}$ .

(Hint :  $D(E/K)$  is the conductor of the regular representation; observe for  $b_3)$  that if  $\det_\rho$  is trivial, then, for any subgroup  $H$  of  $G$ ,  $V^H = V$  or  $\text{codim } V^H \geq 2$ ).

$c)$  Prove that  $f(\rho_1 \otimes \rho_2)$  divides  $f(\rho_1)^{n_2} f(\rho_2)^{n_1}$ , and that these 2 ideals are equal if  $f(\rho_1)$  and  $f(\rho_2)$  are coprime.

(Hint: use the inclusion  $V_1^G \otimes V_2^G \subset (V_1 \otimes V_2)^G$ , and the equality  $V_1^G \otimes V_2 = (V_1 \otimes V_2)^G$  if  $G$  acts trivially on  $V_2$ ).

$d)$  Let  $\bar{\rho}$  be the contragredient representation of  $\rho$ . Prove that  $f(\rho \otimes \bar{\rho})$  divides  $f(\rho)^{2(n-1)}$ .

### Exercise 3 : Artin root numbers of tensor products.

$a)$  Let  $K$  be a finite extension of a  $p$ -adic field, and let  $\chi_1, \chi_2$  be two characters on  $G_K = \text{Gal}(\bar{\mathbb{Q}}_p/K)$ . Assume that  $\chi_1$  is unramified (i.e.  $\chi_1$  factors through an unramified extension). Prove the following two formulae:

$$a_1) \quad W(\chi_1 \chi_2) = W(\chi_1)^{\chi_2(1)} W(\chi_2)^{\chi_1(1)} \det_{\chi_1} (f(\chi_2))$$

$$a_2) \quad \tau(\chi_1 \chi_2) = \tau(\chi_1)^{\chi_2(1)} \tau(\chi_2)^{\chi_1(1)} \det_{\chi_1}^{-1} (f(\chi_2))$$



b) Let  $K$  be a number field, and let  $\rho_1$  and  $\rho_2$  be two representations of  $\Omega_K = \text{Gal}(\mathbb{Q}/K)$  with coprime conductors.

Prove the following equality relating Galois Gauss sums and conductors:

$$\tau(\rho_1 \otimes \rho_2) = \tau(\rho_1)^{\rho_2(1)} \tau(\rho_2)^{\rho_1(1)} \det_{\rho_1}^{-1}(\mathfrak{f}(\rho_2)) \det_{\rho_2}^{-1}(\mathfrak{f}(\rho_1)),$$

where  $\bar{\rho}_i$  is the contragredient representation of  $\rho_i$ .

c) Under the assumptions of b), let  $E$  be a finite normal extension of  $K$  with Galois group  $G$  such that  $\rho_1$  and  $\rho_2$  factor through  $G$ . For every real place  $v$  of  $K$ , let  $\sigma_v \in G$  be a real Frobenius substitution and let  $n_i(v)$  be the number of eigenvalues of  $\rho_i(\sigma_v)$  equal to  $-1$ . Prove the formula (cf. Weil, Lecture Notes 189 (1971) p. 152,

lemma B):

$$W(\rho_1 \otimes \rho_2) = \tau(\rho_1)^{\rho_2(1)} \tau(\rho_2)^{\rho_1(1)} \det_{\rho_1}(\mathfrak{f}(\rho_2)) \det_{\rho_2}(\mathfrak{f}(\rho_1)) (-1)^{\sum_{v \text{ real}} n_1(v) n_2(v)}$$

Hint. To prove a), one may assume that  $\chi_1$  is irreducible of degree 1. Consider for any finite extension  $F$  of  $K$  the functions  $\chi_2 \rightarrow W(\chi_{1,F} \chi_2)$  and  $\chi_2 \rightarrow W(\chi_2)^{\chi_1(1)} \det_{\chi_1}(N_{F/K}(\mathfrak{f}(\chi_2)))$ , where  $\chi_1$  is a fixed unramified character of  $\Omega_K$  and  $\chi_{1,F}$  is the restriction of  $\det_{\chi_1}$  to  $\Omega_F$ . Show that both functions are invariant under induction from  $\Omega_F$  to  $\Omega_K$ , for any field



$F'$  with  $K \subset F' \subset F$  when  $\chi_2(1) = 0$ , and prove that they are equal when  $\chi_2$  is irreducible of degree 1.

Exercise 4 : Zeta functions with a zero at  $s = \frac{1}{2}$ . (cf.

J.V. Armitage, Invent. Math., 15 (1972),  
199-205).

Let  $K$  be a number field. Denote by  $H_K$  its ideal class group. For a character  $\psi : H_K \rightarrow \mathbb{C}^*$ , let  $\psi' : \Omega_K \rightarrow \mathbb{C}^*$  be the character which corresponds to  $\psi$  via the Artin map.

a) Let  $\chi$  be a character of  $\Omega_K$ . Prove the formula

$$W(\chi \psi') = W(\chi) W(\psi')^{\chi(1)} \psi(f(\chi))$$

(Use exercise 3).

b) Let  $E$  be a finite normal extension of  $K$  with Galois group  $G$  and let  $\chi$  be a real valued character of  $G$  such that  $W(\chi) = -1$ . Prove that the function  $s \mapsto L(s, \chi)$  has a zero or a pole of odd order at  $s = \frac{1}{2}$ .

c) Under the assumption of b), prove that the zeta function of  $E$  has a zero at  $s = \frac{1}{2}$ .

d) Let  $\chi$  be a real valued character. Assume that the class in  $H_K$  of  $f(\chi)$  is not a square. Prove that the zeta function of  $E$  or of some quadratic extension of  $E$  has a zero at  $s = \frac{1}{2}$ .

e) Use a) together with the theorem of Fröhlich and Queyrut to prove that the class in  $H_K$  of the conductor of an orthogonal representation is a square (cf. III, cor. 4.2).

Note. The proof of c) runs as follows : by Artin's induction theorem, there exist a positive integer  $N$ , cyclic subgroups  $H_i$  ( $1 \leq i \leq r$ ), integers  $n_i$  ( $1 \leq i \leq r$ ) and irreducible characters of degree one  $\phi_i$  of  $H_i$  for some integer  $r$  such that  $N\chi = \sum_{i=1}^r n_i \text{Ind}_{H_i}^G(\phi_i)$ .

We thus have the equality  $L(s, \chi)^N = \prod_{i=1}^r L(s, \phi_i)^{n_i}$ . Since the  $L$  functions  $s \rightarrow L(s, \phi_i)$  are holomorphic at  $s = \frac{1}{2}$ , one of them has a zero at  $s = \frac{1}{2}$ . We have thus proved the existence of a cyclic subgroup  $H$  of  $G$  and of an irreducible degree 1 character  $\phi$  of  $H$  such that  $L(\frac{1}{2}, \phi) = 0$ . Write now the zeta function of  $E$  as a product  $\zeta_E(s) = L(s, \phi) \prod_{\psi \neq \phi} L(s, \psi)$  where  $\psi$  runs through the irreducible degree 1 characters of  $H$ . Then,  $L(s, \psi)$  is holomorphic at  $s = \frac{1}{2}$  for every  $\psi$ . Since  $L(\frac{1}{2}, \phi) = 0$ ,  $\zeta_E(\frac{1}{2}) = 0$ , Q.E.D.

Exercise 5 : Simple zeros of zeta functions (cf. Stark, Invent. Math., 23 (1974), §3, p.144).

Let  $K$  be a number field and let  $E$  be a finite normal extension of  $K$  with Galois group  $G$ . Let  $s \in \mathbb{C}$ . For any

virtual character  $\chi$  of  $G$ , let  $v_s(\chi)$  be the order at  $z = s$  of the L-function  $z \rightarrow L(z, \chi)$ . Since the function  $\chi \rightarrow v_s(\chi)$  is additive and takes integral values, there exists a virtual character  $\psi_s^G \in R_G$  such that

$$v_s(\chi) = \langle \chi, \psi_s^G \rangle \quad \text{for every } \chi \in R_G.$$

a) Prove that for any subgroup  $H$  of  $G$ ,  $\psi_s^H$  is the restriction of  $\psi_s^G$  to  $H$ .

Assume now that  $s$  is a simple zero of the zeta function of  $E$ .

b) Prove that  $\psi_s^G$  is an irreducible character of degree 1 of  $G$ ; hence, for any representation of  $G$ , the corresponding L-function is holomorphic at  $s$ .

(Hint : prove first the result for  $\psi_s^H$  where  $H$  is a cyclic subgroup of  $G$ . Then, show that it implies the equality  $\langle \psi_s^G, \psi_s^G \rangle_G = 1$ . Therefore,  $\psi_s^G$  is irreducible, and the result follows from the equality  $\psi_s^G(1) = 1$ .)

c) Let  $K_s$  be the cyclic extension of  $K$  corresponding to  $\text{Ker } \psi_s$ . Show that the zeta function of a field  $F$  between  $K$  and  $E$  has a zero at  $s$  if and only if  $F \supset K_s$ .

d) Assume that  $s$  is real. Show that  $\psi_s^G$  takes its values in  $\{\pm 1\}$ ; thus,  $K_s = K$  or  $[K_s : K] = 2$ .

Exercise 6 : Normal extensions with Galois group  $A_5$  (cf.

E. Artin, Collected papers n° 2 and 3).

a) Prove that the alternating group on 5 letters of order 60 has 5 irreducible characters  $\chi_1, \chi_3, \chi'_3, \chi_4, \chi_5$  of respective degrees 1, 3, 3, 4, 5.

(Remark :  $\chi_3$  and  $\chi'_3$ , are conjugate and take their values in  $\mathbb{Q}(\sqrt{5})$ ; they come from icosahedral representations

$A_5 \rightarrow SO_3(\mathbb{R})$ . The character  $\chi_4$  comes from the simplex representation  $A_5 \rightarrow SO_4(\mathbb{R})$ .)

b) Prove that  $\chi_3 + \chi'_3$ ,  $1 + \chi_4$  and  $\chi_5$  are monomial.

Hence, the L-functions  $L(s, \chi_3 + \chi'_3)$ ,  $L(s, \chi_5)$  and  $\zeta_{\mathbb{Q}}(s) L(s, \chi_4)$  are holomorphic (the last one for  $s \neq 1$  only).

It is not known whether  $L(s, \chi_3)$ ,  $L(s, \chi'_3)$  and  $L(s, \chi_4)$  are holomorphic.

Exercise 7 : Dihedral and quaternion extensions (cf. Fröhlich,

Proc. London Math. Soc. 28 (1974), 402-438).

Let  $K$  be a local field, and let  $E$  be a quadratic extension of  $K$  corresponding to a character  $\varepsilon: K^* \rightarrow \{\pm 1\}$ .

Let  $F$  be a cyclic extension of degree  $N$  of  $E$ , corresponding to a character  $\phi: E^* \rightarrow \mathbb{C}^*$ .

a) Prove that  $F/K$  is normal if and only if  $\text{Ker } \phi$  is invariant under the action of  $g = \text{Gal}(E/K)$ .

Assume now that  $F/K$  is normal with Galois group  $G$ . Let  $H = \text{Gal}(F/E)$ .

b) Prove that the non trivial element of  $g = G/H$  acts on  $H$  by  $s \mapsto s^{-1}$  if and only if  $\Phi(N_{E/K}(E^*)) = \{1\}$ , i.e.  $\Phi(\text{Ker } \varepsilon) = \{1\}$ .

c) Assume that  $\Phi(\text{Ker } \varepsilon) = \{1\}$ . Prove that

(i) either  $\Phi$  has a trivial restriction to  $K^*$ , and then  $G$  is dihedral

(ii) or the restriction of  $\Phi$  to  $K^*$  is equal to  $\varepsilon$ , and  $G$  is quaternion.

d) State and prove the corresponding results in the global case.

(Hint : for c), consider the transfer from  $G^{\text{ab}}$  to  $H$ ).

### Exercise 8 : Quasi-finite residue fields.

a) Let  $k$  be a field. Show that there exists an extension  $k_1$  of  $k$  which is a quasi-finite field. (Hint : let  $\bar{k}$  be an algebraic closure of  $k$ ; show the existence of a normal extension  $k'$  of  $\bar{k}(t)$  with Galois group isomorphic to  $\hat{\mathbb{Z}}$ , and use the method of Corps Locaux, ch. XIII. §2, Exer. 3a); hence, one can take for  $k_1$  a field of transcendence degree at most 1 over  $k$ .)

b) Let  $K$  be a local field with residue field  $k$ , and let  $L$  be a totally ramified extension of  $K$ . Let  $k_1$  be an extension of  $k$ . Show the existence of local field  $K_1$  with residue field  $k_1$  which is an extension of  $K$  and is linearly disjoint over  $K$  with  $L$ , i.e. :  $L_1 = L \otimes_K K_1$  is a field.  
(Hint : reduce to the case when  $k_1$  is generated over  $k$  by a single element).

c) Combine a) and b) to prove the following "meta-theorem" : every statement about the ramification groups of a normal totally ramified extension of a local field which is true in the case when the residue fields are quasi-finite is true in general.

d) Application : prove Serre's theorem on conductors in full generality (cf. III, theorem 4.1 and Remark 4.2).





## Local constants

J. T. Tate

(prepared in collaboration with C.J. Bushnell & M.J. Taylor)

Introduction

Notations

§1 Abelian Root Numbers

§2 Existence of Local Constants

§3 Root Numbers of Orthogonal Representations

These notes are intended as an introduction to the theory of non-abelian "local constants" or "root numbers". In the spirit of the Durham conference we treat only the number field case and concentrate on representations of Galois groups rather than of Weil groups. However, the discussion goes over almost without change to the function field case once we fix an additive character for the ground field; and at the end of §2 we have indicated how to pass from Galois groups to Weil groups in the non-Archimedean local case.

Langlands' ideas on the correspondence between representations  $\rho$  of degree  $n$  of Galois groups and automorphic representations of  $GL(n)$  led him to conjecture that the constant  $W(\rho)$  in the functional equation for an Artin L-series  $L(s, \rho)$  could be canonically factored into a product of "local constants"  $W(\rho_v)$ . He announced his proof of the existence of these local constants in [L] but never published it. Deligne [D] found a short global proof for this local existence theorem and our proof in §2 is a variant of Deligne's.

In §1 we prepare the way for this proof by recalling the explicit formulas for the local abelian root numbers  $W(\chi)$  and deriving some properties of them. The property needed for Deligne's proof is that, if  $K$  is a non-Archimedean local field, then for each fixed character  $\alpha$  of  $K^\times$  there are elements  $c_\alpha \in K^\times$  such that  $W(\beta\alpha) = \beta(c_\alpha)W(\alpha)$  for all characters  $\beta$  whose ramification is relatively small compared with that of  $\alpha$ , and that for a finite extension  $L/K$  one can take  $c_\alpha \circ N_{L/K} = c_\alpha$  if one interprets "relatively small" sufficiently strictly for characters  $\beta$  of  $L^\times$ .

In §2 after proving the existence of the local non-abelian root numbers  $W(\rho)$  we derive as corollaries several of their properties. Corollary 5 (ii) gives a global

application, a formula for the global root number  $W(\rho \otimes \sigma)$  when  $\rho$  and  $\sigma$  are two representations of a global Galois group with relatively prime conductors. When  $\rho$  and  $\sigma$  are of degree 2 and 1 respectively, this is the property referred to by Serre just before Theorem 1 of his article in this volume, the property which is needed to get that theorem by Weil's methods.

In §3 we discuss orthogonal (i.e. real) representations and prove the theorem of Fröhlich and Queyrut to the effect that the global root number of such a representation is 1. We also describe how Deligne has given a local explanation of this result in terms of Stiefel-Whitney classes.

### Notations

If  $K$  is a non-Archimedean local field of characteristic 0,  $K/\mathbb{Q}_p$  say, we adopt the following standard notations:

$\mathcal{O}_K$  = the discrete valuation ring in  $K$ ;

$\mathfrak{p}_K$  = the maximal ideal of  $\mathcal{O}_K$ ;

$\psi_K$  = the "canonical" character of the additive group  $K^+$ :

$$\psi_K = \psi_{\mathbb{Q}_p} \circ \text{Tr}_{K/\mathbb{Q}_p}$$

where  $\text{Tr}$  denotes the trace, and  $\psi_{\mathbb{Q}_p}$  is the composition of

the canonical maps:

$$\mathbb{Q}_p \rightarrow \mathbb{Q}_p / \mathbb{Z}_p \rightarrow \mathbb{Q} / \mathbb{Z} \xrightarrow{e^{2\pi i}} \mathbb{R} / \mathbb{Z} \rightarrow S^1,$$

where  $S^1$  denotes the unit circle in  $\mathbb{C}$ .

If  $k$  is an algebraic number field, and  $v$  is a place of  $k$ :

$k_v$  = the completion of  $k$  at  $v$ ;

$\mathcal{O}_v = \mathcal{O}_{k_v}$ ;

$J_k$  = the idele group of  $k$ ;

$C_k$  = the idele class group of  $k$ .

### §1. Root Numbers in the Abelian Case

Let  $\bar{\mathbb{Q}}$  be an algebraic closure of the rational field  $\mathbb{Q}$ , and  $k \subset \bar{\mathbb{Q}}$  an algebraic number field (of finite degree over  $\mathbb{Q}$ ). Let  $\Omega_k = \text{Gal}(\bar{\mathbb{Q}}/k)$ , and let

$$\chi: \Omega_k \rightarrow \mathbb{C}^\times$$

be a continuous 1-dimensional linear representation of  $\Omega_k$ .

Then  $\chi$  factors through  $\Omega_k^{\text{ab}}$ , the Galois group of the maximal abelian extension of  $k$ , and the image of  $\chi$  is a finite subgroup of  $S^1$ . Composing with the Artin reciprocity map

$C_k \rightarrow \Omega_k^{\text{ab}}$ , and the canonical quotient  $J_k \rightarrow C_k$ , we obtain

characters of finite order of the locally compact abelian

groups  $C_k$  and  $J_k$ , which we denote also by  $\chi$ :

$$\chi: C_k \rightarrow S^1,$$

$$\chi: J_k \rightarrow S^1.$$

To the representation  $\chi$  of  $\Omega_k$ , we can attach  $\Lambda(s, \chi)$ , the Artin L-function with factors corresponding to the Archimedean primes of  $K$  ([Dur.M]). This function is the same as the "abelian" L-function attached to the idele-class character  $\chi$  ([T] or [W]), and it satisfies the functional equation:

$$\Lambda(1-s, \chi) = W(\chi) \Lambda(s, \bar{\chi}),$$

where  $W(\chi) \in \mathbb{C}^\times$  is a constant. The root number  $W(\chi)$  may be determined locally in this case. Viewing  $\chi$  as a character of  $J_k$ , let  $\chi_v = \chi|_{k_v^\times}$ , for each place  $v$  of  $k$ . Then (cf. [T] or [W]),

$$W(\chi) = \prod_v W(\chi_v),$$

where the constants  $W(\chi_v)$  depend only on  $k_v$  and  $\chi_v$ , and are given by explicit formulas which we now recall.

Let  $K$  be a local field of characteristic 0, and  $\alpha$  a character of  $K^\times$  of finite order. Then the root number  $W(\alpha)$  is a complex number of absolute value 1, and its precise value is:

$$(i) \quad K = \mathbb{C}, \quad W(\alpha) = 1.$$

(ii)  $K = \mathbb{R}$ ,

$$W(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is trivial,} \\ -i & \text{otherwise, i.e. if} \\ & \alpha(x) = \text{sgn}(x). \end{cases}$$

(iii)  $K$  non-Archimedean: Let  $\mathfrak{f}(\alpha)$  be the conductor of  $\alpha$ ,  $\mathcal{D}_K$  the absolute different of  $K$ ,  $\mathcal{D}(\alpha) = \mathfrak{f}(\alpha)\mathcal{D}_K$ , and  $d \in K$  such that  $d\mathcal{O}_K = \mathcal{D}(\alpha)$ . Let  $\psi_K$  be the canonical character of  $K^+$  defined above. Then:

$$W(\alpha) = N\mathfrak{f}(\alpha)^{-1/2} \sum_{\substack{x \in \mathcal{O}_K \\ \text{mod } \mathfrak{f}(\alpha)}} \bar{\alpha}(d^{-1}x) \psi_K(d^{-1}x).$$

Here,  $N$  denotes the absolute norm, and the sum is taken over a set of representatives of the cosets of  $1 + \mathfrak{f}(\alpha)$  in  $\mathcal{O}_K^\times$  (with the convention  $1 + \mathfrak{f}(\alpha) = \mathcal{O}_K^\times$  if  $\mathfrak{f}(\alpha) = \mathcal{O}_K$ ). In the notation of [Dur.M]:

$$W(\alpha) = N\mathfrak{f}(\alpha)^{-1/2} \tau(\bar{\alpha}).$$

Notice that if  $\alpha$  is non-ramified,  $W(\alpha) = \alpha(\mathcal{D}_K)$ .

Proposition 1 Let  $K$  be a non-Archimedean local field of characteristic 0, and let  $\alpha$  be a character of  $K^\times$  of finite

order. Let  $a$  be an ideal of  $\mathcal{O}_K$  such that  $a^2 \nmid \mathfrak{f}(\alpha)$ , and let  $b = a^{-1} \mathfrak{f}(\alpha)$ . Then there exists  $c \in K$  such that:

$$(i) \quad c\mathcal{O}_K = \mathcal{D}(\alpha), \quad \text{and}$$

$$(ii) \quad \alpha(1+y) = \psi_K(c^{-1}y) \text{ for all } y \in b.$$

Further, for any such  $c$ :

$$(iii) \quad W(\alpha) = N(ba^{-1})^{-1/2} \sum_{\substack{x \in (1+a) \\ \text{mod } b}} \bar{\alpha}(c^{-1}x) \psi_K(c^{-1}x).$$

Proof If  $a = \mathcal{O}_K$ , then  $b = \mathfrak{f}(\alpha)$ , and the assertion (iii) is just the formula above for  $W(\alpha)$ , if  $c$  is any element of  $K$  satisfying (i). Further, any  $c$  satisfying (i) also satisfies (ii), in this case.

Suppose  $a \neq \mathcal{O}_K$ . Then  $p_K | a | b | \mathfrak{f}(\alpha)$ , and if  $y, y' \in b$ , then  $yy' \in \mathfrak{f}(\alpha)$  so that:

$$\alpha(1+y)\alpha(1+y') = \alpha(1+y+y').$$

That is,  $y \mapsto \alpha(1+y)$  is a character of the additive group  $b$ .

This character extends to a character of  $K^+$  and, by local additive duality, there is some  $c \in K$  such that

$$\alpha(1+y) = \psi_K(c^{-1}y) \text{ for all } y \in b. \quad \text{The character}$$

$y \mapsto \psi_K(c^{-1}y)$  of  $K^+$  is trivial on  $\mathfrak{f}(\alpha)$ , but not on

$p_K^{-1} \mathfrak{f}(\alpha) \subset b$ . The character  $\psi_K$  is trivial on  $\mathcal{D}_K^{-1}$ , but not



on  $p_K^{-1} \mathcal{O}_K^{-1}$ . Therefore  $c\mathcal{O}_K = \mathcal{O}(\alpha)$ .

Now:

$$\begin{aligned}
 & \sum_{\substack{x \in \mathcal{O}_K^\times \\ \text{mod } \mathfrak{f}(\alpha)}} \alpha(c^{-1}x) \psi_K(c^{-1}x) \\
 = & \sum_{\substack{z \in \mathcal{O}_K^\times \\ \text{mod } b}} \sum_{\substack{y \in b \\ \text{mod } \mathfrak{f}(\alpha)}} \bar{\alpha}(c^{-1}z(1+y)) \psi_K(c^{-1}z(1+y)) \\
 = & \sum_z [\bar{\alpha}(c^{-1}z) \psi_K(c^{-1}z) \sum_y \psi_K(c^{-1}y(z-1))]
 \end{aligned}$$

by the construction of  $c$ . However, the inner sum is zero unless  $y \mapsto \psi_K(c^{-1}y(z-1))$  is the trivial character of the group  $b/\mathfrak{f}(\alpha)$ ; that is, unless  $z \equiv 1 \pmod{a}$ . So this double sum reduces to:

$$Na \sum_{\substack{z \in (1+a) \\ \text{mod } b}} \bar{\alpha}(c^{-1}z) \psi_K(c^{-1}z),$$

and the assertion (iii) follows.

Corollary 1 (Lamprecht, Dwork) If either  $\alpha$  is non-ramified, or  $p_K^2 \nmid \mathfrak{f}(\alpha)$  (i.e.  $\alpha$  is "truly wildly ramified"),

then  $W(\alpha)$  is a root of unity.

Proof If  $\mathfrak{f}(\alpha) = a^2$ , for some ideal  $a \subset \mathfrak{o}_K$ , then  $a = b$

and

$$W(\alpha) = \bar{a}(c^{-1})\psi_K(c^{-1}),$$

which is clearly a root of unity.

Now assume that  $\mathfrak{f}(\alpha) = a^2 p_K$ , for some proper ideal  $a$  of  $\mathfrak{o}_K$ . Let  $p$  be the residual characteristic of  $K$ . In the Proposition, we have  $b = ap_K$ , and

$$W(\alpha) = Np_K^{-1/2} \sum_{\substack{x \in (1+a) \\ \text{mod } \mathfrak{p}_K}} \bar{a}(c^{-1}x)\psi_K(c^{-1}x).$$

Since  $a$  is a proper ideal of  $\mathfrak{o}_K$ , the group  $(1+a)/(1+\mathfrak{f}(\alpha))$  is a  $p$ -group and so  $\bar{a}(x)$ , for  $x \in (1+a)$ , is a  $p$ -power root of unity. Also, the values of  $\psi_K$  are  $p$ -power roots of unity. Hence the quantity  $\zeta = (\alpha(c^{-1})W(\alpha))^2$  lies in the field  $E$  of  $p^N$ -th roots of unity, for some  $N$ . We must show that  $\zeta$  is a root of unity. Since the field  $E$  has only one place above  $p$ , this will follow if we show that  $\|\zeta\|_v = 1$  for each place  $v$  of  $E$  which is not above  $p$ .

This is a consequence of:

Lemma Let  $E$  be a subfield of  $\mathbb{C}$  containing  $W(\alpha)$ . Then  $\|W(\alpha)\|_v = 1$  for each place  $v$  of  $E$  not dividing  $p$ , the residual characteristic of  $K$ .

Proof Suppose that  $v$  is non-Archimedean (and does not divide  $p$ ). The explicit formula for  $W(\alpha)$  shows that  $W(\alpha)$  is a local integer at  $v$ . One also knows ([Dur.M,2.2]) that:

$$(*) \quad W(\alpha)W(\bar{\alpha}) = \alpha(-1),$$

so that  $W(\alpha)$  is a local unit at  $v$ , i.e.  $\|W(\alpha)\|_v = 1$ .

Suppose that  $v$  is Archimedean. The ratio  $W(\alpha)^\sigma / W(\alpha^\sigma)$  is a root of unity for every automorphism  $\sigma$  of  $\mathbb{C}$  (cf. [Dur.M,5.1]). Choosing  $\sigma$  so that  $\|x\|_v = |x^\sigma|$  (ordinary absolute value), we have  $\|W(\alpha)\|_v = |W(\alpha^\sigma)|$  and we know  $|W(\alpha^\sigma)| = 1$ .

Corollary 2 Let  $\beta$  be a character of  $K^\times$  of finite order such that  $\beta(\beta) | \alpha$ . Then:

$$W(\beta.\alpha) = \beta(c)W(\alpha).$$

In particular, if  $\beta$  is non-ramified,  $W(\beta.\alpha) = \beta(\mathcal{D}(\alpha))W(\alpha)$ .

Proof The hypothesis implies that either  $p_K \nmid \beta(\beta) | \beta(\alpha)$  or

else both  $\alpha$  and  $\beta$  are non-ramified. Hence  $\mathfrak{f}(\beta.\alpha) = \mathfrak{f}(\alpha)$ .

So, from the Proposition applied to  $\beta\alpha$  instead of  $\alpha$ , we have:

$$W(\beta.\alpha) = N(ba^{-1})^{-1/2} \sum_{\substack{x \in (1+a) \\ \text{mod } b}} \overline{\beta\alpha}(c^{-1}x) \psi_K(c^{-1}x).$$

For any  $x \equiv 1 \pmod{a}$ , we have  $\overline{\beta\alpha}(c^{-1}x) = \beta(c)\overline{\alpha}(c^{-1}x)$ , and the Corollary follows.

When we have an extension  $L/K$  and an ideal  $a$  of  $\mathcal{O}_K$ ,  $a\mathcal{O}_L$  is an ideal of  $\mathcal{O}_L$  which we shall again denote by  $a$  when there is no fear of confusion.

Corollary 3 Let  $L/K$  be a finite extension with relative different  $\mathcal{D}_{L/K}$ . Suppose the ideal  $a$  satisfies:

(a)  $p_K | a$  if  $L/K$  is ramified, and

(b)  $a^2 \mathcal{D}_{L/K}^2 | \mathfrak{f}(\alpha)$ .

Let  $\beta$  be a character of  $L^\times$  of finite order such that  $\mathfrak{f}(\beta) | a$ , and let  $\alpha_L$  denote the character  $x \mapsto \alpha(N_{L/K}(x))$  of  $L^\times$ . Then if  $c \in K$  is as in the Proposition,

$$W(\beta.\alpha_L) = \beta(c)W(\alpha_L).$$

Proof This Corollary will follow from Corollary 2, applied to the field  $L$  and the characters  $\alpha_L$  and  $\beta$  of  $L^\times$ , once we show that in Proposition 1 we can replace  $K$ ,  $\alpha$ , and  $a$  by  $L$ ,  $\alpha_L$ , and  $a\alpha_L$ , and still keep the same  $c$ .

Suppose first  $a = \alpha_K$ . Then we have only to verify that  $c\alpha_K = \mathcal{D}(\alpha)$  implies that  $c\alpha_L = \mathcal{D}(\alpha_L)$ , i.e. that  $\mathcal{D}(\alpha_L) = \mathcal{D}(\alpha)$ . Since  $L/K$  is non-ramified in this case, there is no problem. (We have  $\mathcal{D}_L = \mathcal{D}_K$  and, since  $N_{L/K}$  maps  $1 + \mathfrak{p}_L^n$  onto  $1 + \mathfrak{p}_K^n$ , also  $\mathfrak{f}(\alpha_L) = \mathfrak{f}(\alpha)$ .)

Assume now  $p_K | a$ . Let  $y \in a^{-1}\mathcal{D}_{L/K}^{-1}\mathfrak{f}(\alpha) = b\mathcal{D}_{L/K}^{-1}$ . Then  $\text{Tr}_{L/K}(y) \in b$ , and the product of any two conjugates of  $y$  over  $K$  is divisible by  $a^{-2}\mathcal{D}_{L/K}^{-2}\mathfrak{f}(\alpha)^2$  and hence by  $\mathfrak{f}(\alpha)$ . It follows that

$$\begin{aligned}
 (*) \quad \alpha_L(1+y) &= \alpha(N_{L/K}(1+y)) = \alpha(1+\text{Tr}_{L/K}(y)) = \psi_K(c^{-1}\text{Tr}_{L/K}(y)) \\
 &= \psi_L(c^{-1}y), \quad \text{for all } y \in a^{-1}\mathcal{D}_{L/K}^{-1}\mathfrak{f}(\alpha).
 \end{aligned}$$

Using  $\mathcal{D}_L = \mathcal{D}_{L/K}\mathcal{D}_K$ , and  $p_K | a$ , it is easy to see that (\*) implies  $\mathfrak{f}(\alpha_L) = \mathcal{D}_{L/K}^{-1}\mathfrak{f}(\alpha)$ , and  $c\alpha_L = \mathcal{D}(\alpha_L)$ . That being so, (\*) shows that  $c$  satisfies (ii) of Proposition 1 for the field  $L$ , the character  $\alpha_L$ , and the ideal  $a\alpha_L$ , as was to be shown.

## §2. Existence of Local Constants

Throughout this section, we consider only local and global fields of characteristic zero. If  $K$  is such a field, and  $\bar{K}$  is an algebraic closure of  $K$ , then for any finite extension  $L/K$ ,  $L \subset \bar{K}$ , we write  $\Omega_L = \text{Gal}(\bar{K}/L)$ .

If  $G$  is a profinite group, a virtual representation of  $G$  is an element of the free abelian group on the set of isomorphism classes of irreducible continuous finite-dimensional complex linear representations of  $G$ . If  $K$  is a local or global field, let  $R(K)$  denote the set of pairs  $(L, \rho)$ , where  $K \subset L \subset \bar{K}$ ,  $L/K$  is finite, and  $\rho$  is a virtual representation of  $\Omega_L$ .

If  $E/K$  is a finite Galois extension contained in  $\bar{K}/K$ ,  $R(E/K)$  denotes the set of pairs  $(L, \rho)$ , where  $K \subset L \subset E$ , and  $\rho$  is a virtual representation of  $\text{Gal}(E/L)$ . In a natural way, we may regard  $R(E/K)$  as a subset of  $R(K)$ , and then:

$$R(K) = \bigcup_{E/K} R(E/K)$$

as  $E$  ranges over all finite Galois extensions of  $K$  in  $\bar{K}$ .

Let  $R_1(K)$  denote the set of pairs  $(L, \chi)$ , where  $L$  is a finite extension of  $K$  in  $\bar{K}$ , and  $\chi$  is a character of finite order of  $L^\times$  (if  $K$  is local) or  $C_L$  (if  $K$  is global). Via

class field theory, we may view  $R_1(K)$  as a subset of  $R(K)$ . We also write  $R_1(E/K) = R_1(K) \cap R(E/K)$ .

Suppose we have a function  $F$  defined on  $R_1(K)$  taking values in some abelian group  $A$ . We say  $F$  is extendible if  $F$  can be extended to an  $A$ -valued function on  $R(K)$  satisfying:

- (a)  $F(L, \rho_1 + \rho_2) = F(L, \rho_1) \cdot F(L, \rho_2)$  for all  $(L, \rho_i) \in R(K)$ , and  
 (b) if  $(L, \rho) \in R(K)$  with  $\dim(\rho) = 0$ , and  $L \supset L' \supset K$ , then:

$$F(L, \rho) = F(L', \text{Ind}_{L/L'}(\rho)),$$

where  $\text{Ind}_{L/L'}(\rho)$  is the virtual representation of  $\Omega_L$ , induced from  $\rho$ .

If  $E/K$  is finite Galois, we say  $F$  is extendible in  $E/K$  if  $F$  can be extended to a function on  $R(E/K)$  satisfying (a) and (b) with  $(L, \rho_i)$  and  $(L, \rho)$  in  $R(E/K)$ .

Remarks 1) If  $F$  is extendible (or extendible in  $E/K$ ), there is a unique extension of  $F$  to  $R(K)$  (or  $R(E/K)$ ) satisfying (a) and (b). For, suppose we have two such extensions  $F_1$  and  $F_2$ . Then, if  $(L, \rho) \in R(E/K)$ :

$$F_i(L, \rho) = F_i(L, \rho - \dim(\rho)[1_L]) \cdot F(L, [1_L])^{\dim(\rho)}, \text{ for } i = 1, 2,$$

where  $[1_L]$  denotes the unit representation of  $\text{Gal}(E/L)$ . By



Brauer induction ([S,p.96 Ex.2]):

$$\rho - \dim(\rho)[1_L] = \sum_i n_i \text{Ind}_{L_i/L}(\chi_i - [1_{L_i}])$$

for some rational integers  $n_i$  and some  $(L_i, \chi_i) \in R_1(E/L)$ .

Consequently:

$$\begin{aligned} F_1(L, \rho - \dim(\rho)[1_L]) &= \prod_i F(L_i, \chi_i)^{n_i} F(L_i, [1_{L_i}])^{-n_i} \\ &= F_2(L, \rho - \dim(\rho)[1_L]), \end{aligned}$$

and therefore  $F_1 = F_2$ .

2) By the uniqueness just proved, it is clear that  $F$  is extendible if and only if it is extendible in  $E/K$  for all  $E$ .

3) Suppose  $F$  is extendible and let  $F$  denote its extension. In the situation of (b), but without the hypothesis  $\dim(\rho) = 0$ , we have:

$$F(L', \text{Ind}_{L/L'}(\rho)) = \lambda_{L/L'}(F)^{\dim(\rho)} F(L, \rho),$$

where:

$$\lambda_{L/L'}(F) = \frac{F(L', \text{Ind}_{L/L'}[1_L])}{F(L, [1_L])}$$

is a constant depending only on  $F$ , and on the extension  $L/L'$ . Indeed, this formula follows immediately on writing  $\rho = \rho_0 + \dim(\rho)[1_L]$ , where  $\dim(\rho_0) = 0$ , and applying (a)

and (b). If  $\lambda_{L/L'}(F) = 1$  for all  $L/L'$ , i.e., if (b) holds without the hypothesis  $\dim(\rho) = 0$ , then we shall call  $F$  strongly extendible.

Examples (I) If  $K$  is global,  $(L, \chi) \mapsto \Lambda(s, \chi)$  is strongly extendible. The extension  $(L, \rho) \mapsto \Lambda(s, \rho)$  is given by Artin's theory of non-abelian  $L$ -series.

(II) If  $K$  is global or local non-Archimedean,  $(L, \chi) \mapsto N_{L/K}(\zeta(\chi))$  is extendible. The extension is  $(L, \rho) \mapsto N_{L/K}(\zeta(\rho))$ , where  $\zeta(\rho)$  is the Artin conductor of  $\rho$ . In the sense of Remark 3), we have in this case

$\lambda_{L/L'} = N_{L'/K}(d_{L/L'})$ , where  $d$  denotes the discriminant.

(III) If  $c \in C_K$  ( $K$  global) or  $c \in K^\times$  ( $K$  local), then  $(L, \chi) \mapsto \chi(c)$  is extendible by  $(L, \rho) \mapsto \det_\rho(c)$ . Here we view  $c \in C_L$  or  $L^\times$  via the canonical inclusions  $C_K \hookrightarrow C_L$  or  $K^\times \hookrightarrow L^\times$ . In this case we have  $\lambda_{L/L'} = \varepsilon_{L/L'}(c) = \pm 1$ , where  $\varepsilon_{L/L'}$  is the character corresponding by class field theory to the extension  $L'(\sqrt{d})/L'$ , where  $d$  is the discriminant of  $L/L'$ .

(IV) Suppose that  $F(L, \chi)$  depends only on  $L$ ,  $F(L, \chi) = a(L)$ , say. Then  $F$  is extendible by  $F(L, \rho) = a(L)^{\dim(\rho)}$ .

(V) If  $K$  is global,  $(L, \chi) \mapsto W(\chi)$  is strongly extendible by  $(L, \rho) \mapsto W(\rho) = \Lambda(1-s, \rho) \Lambda(s, \bar{\rho})^{-1}$ .

Notice also that a product of extendible functions with values in the same group  $A$  is extendible.

Theorem 1 (Langlands) If  $K$  is a local field of characteristic zero (\*), then  $(L, \chi) \mapsto W(\chi)$  is extendible.

This result was proved, up to sign, by Dwork [Dw]; see Corollary 2 below.

The proof we give of Theorem 1 is a modified version of that of Deligne [D]. In the terminology of [D], our local  $W(\rho)$  is  $\mathfrak{E}(\rho, \psi_K, dx, \frac{1}{2}) = \mathfrak{E}(\rho \omega_{\frac{1}{2}}, \psi_K, dx)$ , where  $dx$  is the Haar measure on  $K^+$  which is self-dual with respect to  $\psi_K$ .

When  $K$  is an Archimedean local field, all irreducible representations of  $\Omega_K$  are 1-dimensional, and the theorem is easily checked. So let  $E/K$  be a finite Galois extension of non-Archimedean local fields. We wish to prove that  $(L, \chi) \mapsto W(\chi)$  is extendible in  $E/K$ .

---

(\*) The restriction to characteristic 0 is just to fix ideas; the result is true, and can be proved in essentially the same way, in any characteristic.

Lemma There exists a finite Galois extension  $e/k$  of global fields and a place  $v_0$  of  $k$  such that:

(i) there is a unique place  $u_0$  of  $e$  lying over  $v_0$  and the extension  $e_{u_0}/k_{v_0}$  is isomorphic to our given local extension  $E/K$ ;

(ii)  $k$  is totally complex (i.e.  $k$  has no real Archimedean place).

Proof Let  $e'$  be a global field which is dense in  $E$  and which contains some imaginary quadratic subfield of  $K$ . Let  $e$  be the compositum of the fields  $(e')^\sigma$  for  $\sigma \in \text{Gal}(E/K)$ , and let  $k = e \cap K$ . Then  $\text{Gal}(E/K)$  acts on  $e$ , and  $k$  is the fixed field for this action, so  $e/k$  is Galois and we may identify  $\text{Gal}(E/K)$  with  $\text{Gal}(e/k)$ . Since  $k$  contains an imaginary quadratic field, it is totally complex. Let  $v_0$  be the place of  $k$  induced by the inclusion  $k \subset K$ , and let  $u_0$  be the place of  $e$  induced by  $e \subset E$ . Then  $u_0$  is invariant under  $\text{Gal}(e/k)$ , so is the only place of  $e$  above  $v_0$ . The completion  $e_{u_0}$  is  $E$ , since  $e$  was chosen dense in  $E$ . The completion  $k_{v_0}$  is obviously contained in  $K$ , and must be all of  $K$  by comparison of degrees.

Let  $k$ ,  $e$ ,  $v_0$ , and  $u_0$  be as in the lemma. Identifying

$E/K$  with  $e_{u_o}/k_{v_o}$  we have an isomorphism  $\text{Gal}(E/K) \simeq \text{Gal}(e/k)$  and hence a bijection  $(\ell, \rho) \mapsto (\ell_{w_o}, \rho_{w_o})$  between  $R(e/k)$  and  $R(E/K)$ , where  $w_o$  is the unique place of  $\ell$  above  $v_o$ , for  $e \supset \ell \supset k$ , and where  $\rho_{w_o}$  is the restriction of  $\rho$  to  $\text{Gal}(E/\ell_{w_o})$ . Of course, this bijection commutes with addition and induction. Our problem is therefore to prove that the function:

$$(\ell, \chi) \mapsto W(\chi_{w_o}) \quad (\text{the } \underline{\text{local}} \text{ root number})$$

is extendible in  $e/k$ .

If  $e \supset \ell \supset k$  and  $v$  is a place of  $k$ , we write  $u$  and  $w$  for primes of  $e$  and  $\ell$  such that  $u|w|v$ . For each non-Archimedean  $v \neq v_o$ , let  $a_v$  be an ideal of  $\mathcal{O}_v$  such that  $\delta(\beta) | a_v$  for each  $(F, \beta) \in R_1(e_u/k_v)$ , and such that  $a_v = \mathcal{O}_v$  if  $v$  is non-ramified in  $e$  (in which case each  $\beta$  is non-ramified). Let  $\alpha$  be a character of finite order of  $C_k$  such that  $\alpha_{v_o} = 1$ , and such that  $a_v^{2D^2} | \delta(\alpha_v)$  for each non-Archimedean  $v \neq v_o$ . (If  $v$  is non-ramified in  $e$ , this last condition is no condition at all. Thus the requirement on  $\alpha$  is that it be 1 at one place, and highly ramified at a finite set of the remaining places. The existence of such an  $\alpha$  - indeed of an  $\alpha$  having preassigned local components at a finite set of places - is guaranteed by the Grunwald-

Wang theorem, cf. e.g. [AT,p.103,th.5].)

Let  $c = (c_v)$  be an idele of  $k$  constructed as follows:

$c_v = 1$ , if  $v$  is Archimedean or if  $v = v_o$ ;

$c_v$  = the element of  $k_v$  associated to  $\alpha_v$  and  $a_v$  as in

Proposition 1, for non-Archimedean  $v \neq v_o$ .

Let  $(\ell, \chi) \in R_1(e/k)$ , and let  $\alpha_\ell = \alpha \circ N_{\ell/k}$ . Then for each place  $w$  of  $\ell$  we have  $(\alpha_\ell)_w = \alpha_v \circ N_{\ell_w/k_v}$ , and:

$$W(\chi_w \cdot (\alpha_\ell)_w) = \begin{cases} \chi_w(c_v) W((\alpha_\ell)_w) & \text{if } w \text{ is non-Archimedean and } w \neq w_o; \\ W(\chi_{w_o}) & \text{if } w = w_o; \\ 1 & \text{if } w \text{ is Archimedean.} \end{cases}$$

The first case follows from Corollary 3 of Proposition 1, the second from the fact that  $\alpha_{v_o} = 1$ , and the third from the fact that  $k$  is totally complex so  $\alpha_v$  and  $\chi_w$  are 1 for Archimedean  $v$ .

Expressing the global root numbers as a product of local ones, we find:

$$\begin{aligned} W(\chi \alpha_\ell) &= \prod_w W(\chi_w \cdot (\alpha_\ell)_w) \\ &= W(\chi_{w_o}) \cdot \prod_{\substack{w \neq w_o \\ w \text{ non-Arch.}}} \chi_w(c_v) W((\alpha_\ell)_w) \\ &= W(\chi_{w_o}) \chi(c) a(\ell), \end{aligned}$$



where

$$a(\ell) = \prod_{w \neq w_0} W((\alpha_\ell)_w)$$

By example III,  $(\ell, \chi) \mapsto \chi(c)$  is extendible. By example IV,

$(\ell, \chi) \mapsto a(\ell)$  is extendible. By example V,

$(\ell, \chi) \mapsto W(\chi \cdot \alpha_\ell)$  is extendible by  $(\ell, \rho) \mapsto W(\rho \otimes \alpha_\ell)$ ,

because  $\alpha_\ell$  corresponds to the restriction of  $\alpha$  to  $\Omega_\ell$ , and

$\text{Ind}(\rho \otimes \text{res}(\alpha)) = (\text{Ind } \rho) \otimes \alpha$ . Hence:

$$(\ell, \chi) \mapsto W(\chi_{w_0}) = W(\chi \cdot \alpha_\ell) \chi(c)^{-1} a(\ell)^{-1}$$

is extendible, as was to be shown.

Corollary 1 Let  $K$  be a local field of characteristic 0, and let  $(L, \rho) \in R(K)$ . Then:

- (i)  $|W(\rho)| = 1$ ;
- (ii)  $W(\rho)W(\bar{\rho}) = \det_\rho(-1)$ ;
- (iii) if  $\rho = \bar{\rho}$ , then  $W(\rho)$  is a fourth root of unity.

Proof (i) If  $(L, \chi) \in R_1(K)$ , then  $|W(\chi)| = 1$ . Clearly  $(L, \chi) \mapsto |W(\chi)| = 1$  is extendible by  $(L, \rho) \mapsto |W(\rho)|$ .

Hence, by uniqueness of extension,  $|W(\rho)| = 1$ .

(ii) If  $(L, \chi) \in R_1(K)$ , then  $W(\chi)W(\bar{\chi}) = \chi(-1)$ ,

cf. [Dur.M, 2.2].



Now,  $(L, \chi) \mapsto W(\chi)W(\bar{\chi})$  is clearly extendible by  $(L, \rho) \mapsto W(\rho)W(\bar{\rho})$ , so by uniqueness of extension and example III, we have  $W(\rho)W(\bar{\rho}) = \det_{\rho}(-1)$ .

(iii) is now immediate, since  $\det_{\rho}(-1) = \pm 1$ .

Remark Using the lemma which is stated before Corollary 2 of Proposition 1, we can obviously generalise (i) as follows: If  $E$  is any subfield of  $\mathbb{C}$  containing  $W(\rho)$ , then  $\|W(\rho)\|_v = 1$  for every place  $v$  of  $E$  which does not lie above  $p$ , the residual characteristic of  $K$ .

Corollary 2 (Dwork, [Dw]) The function  $(L, \chi) \mapsto \chi(-1)W(\chi)^2$  is strongly extendible on  $R(K)$ .

Indeed, the extension is  $(L, \rho) \mapsto \det_{\rho}(-1)W(\rho)^2$ . By Corollary 1, this is the same as  $W(\rho - \bar{\rho})$ , and since  $\dim(\rho - \bar{\rho}) = 0$ , it is a "strong" extension.

Corollary 3 Let  $K$  be an algebraic number field, and  $(K, \rho) \in R(K)$ . For each place  $v$  of  $K$ , let  $\rho_v$  be the restriction of  $\rho$  to a decomposition group of  $v$ . Then  $(K_v, \rho_v) \in R(K_v)$  and:

$$W(\rho) = \prod_v W(\rho_v).$$

where the product is taken over all places  $v$  of  $K$ .

Proof It follows from the group-theoretic properties of induction and restriction ([S, Prop. 22]) that if  $(L, \theta) \in R(K)$ , and if  $v$  is a place of  $K$ , then:

$$\text{Ind}_{L/K}(\theta)_v = \sum_{w|v} \text{Ind}_{L_w/K_v}(\theta_w),$$

where the sum is taken over all places  $w$  of  $L$  above  $v$ . This implies that  $(L, \theta) \mapsto \prod_w W(\theta_w)$  is an extension of  $(L, \chi) \mapsto \prod_w W(\chi_w)$ ,  $(L, \chi) \in R_1(K)$ . Since  $W(\chi) = \prod_w W(\chi_w)$  for  $(L, \chi) \in R_1(K)$ , the result follows from uniqueness of extension.

Now let  $K$  be a non-Archimedean local field,  $E/K$  a finite Galois extension, and  $\rho: \text{Gal}(E/K) \rightarrow \text{Aut}_{\mathbb{C}}(V)$  a representation of  $\text{Gal}(E/K)$  on a complex vector space  $V$ . Let  $P(E/K)$  denote the first ("wild") ramification group of  $E/K$ , and let  $V^P$  be the subspace of all elements of  $V$  fixed by  $\rho(P(E/K))$ . Then  $\rho$  induces a representation:

$$\rho^P : \text{Gal}(E/K)/P(E/K) \rightarrow \text{Aut}_{\mathbb{C}}(V^P).$$

Notice that for representations  $\rho_1$  and  $\rho_2$  we have

$(\rho_1 + \rho_2)^P = \rho_1^P + \rho_2^P$ , so that  $\rho^P$  is defined even when  $\rho$  is a virtual representation.

Corollary 4 Let  $K$  be a non-Archimedean local field, and let  $(K, \rho) \in R(K)$ . Then:

$$W(\rho)/W(\rho^P)$$

is a root of unity.

Remark Since  $\rho \mapsto \rho^P$  is additive, it is enough to prove the Corollary for irreducible  $\rho$ . If  $\rho$  is irreducible, then either  $\rho^P = \rho$ , in which case the result is trivial, or else  $\rho^P = 0$ , in which case it states that  $W(\rho)$  is a root of unity. That statement is Dwork's [Dw, Th.6(b)]; the version above is Deligne's [D, Appendix].

Proof For two non-zero complex numbers  $a$  and  $b$ , we write  $a \sim b$  if  $ab^{-1}$  is a root of unity.

Lemma 1 Let  $(L, \theta) \in R(K)$ , and suppose  $L \supset L' \supset K$ . Then:

$$W(\theta) \sim W(\text{Ind}_{L/L'}(\theta)).$$

Proof  $W(\theta) \cdot W(\text{Ind}_{L/L'}(\theta))^{-1} = W(\text{Ind}_{L/L'}[1_L])^{-\dim(\theta)}$ , which

is a root of unity by Corollary 1 (iii). (Alternatively, it is obvious from Corollary 2 that  $W(\theta)/W(\text{Ind}(\theta))$  is a fourth root of unity.)

Lemma 2 Let  $(K, \alpha) \in R_1(K)$ , and let  $L/K$  be a totally wildly ramified extension (i.e. the maximal tamely ramified extension of  $K$  in  $L$  is  $K$  itself). If  $\alpha$  is tamely ramified, then:

$$W(\alpha) \sim W(\alpha_L).$$

Proof Recall the notation  $\alpha_L = \alpha \circ N_{L/K}$ . If  $\alpha$  is non-ramified, then  $\alpha_L$  is also, and the assertion is immediate.

So assume that  $\mathfrak{f}(\alpha) = p_K$ . Then  $\mathfrak{f}(\alpha_L) = p_L$ . We can view  $\alpha$  as a character of  $(\mathcal{O}_K/p_K)^\times = \mathcal{O}_K^\times \bmod^\times p_K$ . Then:

$$W(\alpha) \sim N_K^{-1/2} \sum_{\substack{x \in \mathcal{O}_K \\ \bmod^\times p_K}} \bar{\alpha}(x) \lambda(x)$$

for any non-trivial character  $\lambda$  of the additive group

$(\mathcal{O}_K/p_K)^+$ . As  $x$  runs through a set of representatives of  $\mathcal{O}_K^\times \bmod^\times p_K$ , it also runs through a set of representatives of  $\mathcal{O}_L^\times \bmod^\times p_L$ , since  $N_{L/K}(x) = x^{[L:K]}$ , and  $y \mapsto y^{[L:K]}$  is an automorphism of the field  $\mathcal{O}_K/p_K$ . So:

$$\begin{aligned}
 W(\alpha_L) &\sim Np_L^{-1/2} \sum_{\substack{x \in \mathcal{O}_K^\times \\ \text{mod } p_K^\times}} \bar{\alpha}_L(x) \lambda(x^{[L:K]}) \\
 &= Np_K^{-1/2} \sum_x \bar{\alpha}(x^{[L:K]}) \lambda(x^{[L:K]}) \\
 &\sim W(\alpha).
 \end{aligned}$$

By Brauer induction, it is enough to prove the Corollary when  $\rho$  is a representation of  $\text{Gal}(E/K)$  of the form  $\text{Ind}_{L/K}(\chi)$ , for some  $(L, \chi) \in R_1(E/K)$ .

Either:  $\chi^P = 0$ , or  $\chi^P = \chi$ .

In the first case, it follows from [S, Prop. 22] that the restriction of  $\text{Ind}_{L/K}(\chi)$  to  $P(E/K)$  does not contain the unit representation. Therefore  $\text{Ind}_{L/K}(\chi)^P = 0$ , and the result follows from Lemma 1 and Corollary 1 to Proposition 1.

So assume that  $\chi^P = \chi$ . Then  $\chi$  is trivial on  $\text{Gal}(E/L) \cap P(E/K)$ , and we may extend  $\chi$  to a representation of  $\text{Gal}(E/L).P(E/K)$  by giving it the value 1 on  $P(E/K)$ . Call this representation  $\chi'$ , and then by Lemma 2 we have  $W(\chi) \sim W(\chi')$ . The representation  $\text{Ind}_{L/K}(\chi)^P$  contains  $\text{Ind}_{E'/K}(\chi')$ , where  $\text{Gal}(E/E') = \text{Gal}(E/L).P(E/K)$ . Further,

it follows from Frobenius Reciprocity ([S,Th.13]) and the properties of restriction that the unit representation occurs with multiplicity exactly  $[E':K]$  in the restriction of  $\text{Ind}_{L/K}(\chi)$  to  $P(E/K)$ . So  $\text{Ind}_{L/K}(\chi)^P$  and  $\text{Ind}_{E'/K}(\chi')$  have the same degree, and are therefore equal. Hence:

$$W(\rho) \sim W(\chi) \sim W(\chi') \sim W(\text{Ind}_{E'/K}(\chi')) = W(\rho^P).$$

Corollary 5 (i) If  $K$  is local non-Archimedean,

$(K, \rho) \in R(K)$ , and if  $\chi$  is a non-ramified character of  $K^\times$  of finite order, then:

$$W(\chi \otimes \rho) = \chi(\mathfrak{f}(\rho)) \cdot W(\chi)^{\dim(\rho)} W(\rho) = \chi(\mathcal{D}(\rho)) W(\rho),$$

where  $\mathcal{D}(\rho) = \mathfrak{f}(\rho) \mathcal{D}_K^{\dim(\rho)}$ .

(ii) If  $K$  is an algebraic number field, and  $\rho$  and  $\sigma$  are representations of  $\Omega_K$  with relatively prime conductors, then

$$W(\rho \otimes \sigma) = (-1)^a \det_\rho(\mathfrak{f}(\sigma)) \det_\sigma(\mathfrak{f}(\rho)) \cdot W(\rho)^{\dim(\sigma)} W(\sigma)^{\dim(\rho)},$$

where  $a$  is the number of Archimedean primes of  $K$  at which

$\det_\rho$  and  $\det_\sigma$  are both non-trivial.

Remark The symbol  $\det_\rho(\mathfrak{f}(\sigma))$  is to be understood in the sense  $\det_\rho(\mathfrak{f}(\sigma)) = \det_\rho(f)$ , where  $f$  is an idele of  $K$  such that  $f_v = 1$  if  $v$  is Archimedean or if  $\rho$  is ramified at  $v$ ,

and  $f_v \sigma_v = \mathcal{J}(\sigma_v)$  otherwise. Likewise for  $\det_\sigma(\mathcal{J}(\rho))$ .

Proof (i) If  $(L, \alpha) \in R_1(K)$ , then by Proposition 1 Corollary 2, we have  $W(\chi_L \cdot \alpha) = \chi_L(\mathcal{D}(\alpha))W(\alpha)$ . But:

$$\begin{aligned}\chi_L(\mathcal{D}(\alpha)) &= \chi(N_{L/K}(\mathcal{J}(\alpha))) \cdot \chi_L(\mathcal{D}_L) \\ &= \chi(N_{L/K}(\mathcal{J}(\alpha))) \cdot W(\chi_L).\end{aligned}$$

So by Theorem 1 and examples II and IV,  $(L, \alpha) \mapsto W(\chi_L \otimes \alpha)$  is extendible by:

$$(L, \theta) \mapsto \chi(N_{L/K}(\mathcal{J}(\theta))) \cdot W(\chi_L)^{\dim(\theta)} W(\theta).$$

Hence by uniqueness of extension:

$$W(\chi \otimes \rho) = \chi(\mathcal{J}(\rho)) \cdot W(\chi)^{\dim(\rho)} W(\rho).$$

(ii) Suppose that  $v$  is non-Archimedean, and that  $\sigma_v$  is non-ramified. Then  $\sigma_v$  is a sum of one-dimensional representations, all of which are non-ramified, and by (i):

$$W(\rho_v \otimes \sigma_v) = \det_{\sigma, v}(\mathcal{J}(\rho_v)) \cdot W(\rho_v)^{\dim(\sigma)} W(\sigma_v)^{\dim(\rho)},$$

where  $\det_{\sigma, v} = (\det_\sigma)_v$ . At any other non-Archimedean place  $v$ :

$$W(\rho_v \otimes \sigma_v) = \det_{\rho, v}(\mathcal{J}(\sigma_v)) \cdot W(\rho_v)^{\dim(\sigma)} W(\sigma_v)^{\dim(\rho)}.$$

Notice that these expressions are symmetric in  $\rho$  and  $\sigma$  if neither is ramified at  $v$ .



If  $v$  is Archimedean,  $\rho_v$  and  $\sigma_v$  are both sums of one-dimensional representations and one verifies directly that:

$$W(\rho_v \otimes \sigma_v) = (-1)^{a_v} W(\rho_v)^{\dim(\sigma)} W(\sigma_v)^{\dim(\rho)},$$

where  $a_v = 0$  unless both  $\det_{\sigma, v}$  and  $\det_{\rho, v}$  are non-trivial, in which case  $a_v = 1$ . Taking the product over all  $v$ :

$$W(\rho \otimes \sigma) = (-1)^a \cdot \det_{\rho}(\zeta(\sigma)) \det_{\sigma}(\zeta(\rho)) \cdot W(\rho)^{\dim(\sigma)} W(\sigma)^{\dim(\rho)},$$

where  $a = \sum_{v|\infty} a_v$ .

So far, we have constructed  $W(\rho)$  only for representations  $\rho$  of Galois groups, not of Weil groups. We close this section by sketching how one can extend the theory to Weil groups in the non-Archimedean local case. In that case, the basic fact ([D, 4.10]) is that an irreducible representation  $\phi$  of the Weil group is of the form  $\phi = \rho \otimes \omega_s$  for some  $s \in \mathbb{C}$ , where  $\rho$  is an irreducible representation of the Galois group and where  $\omega_s$  is the quasicharacter of the Weil group corresponding to the quasicharacter  $x \mapsto \|x\|_K^s$  of  $K^\times$ . (Here,  $\|x\|_K$  is the normalised absolute value function on our local field  $K$ .)

Furthermore, we have  $\rho \otimes \omega_s = \rho' \otimes \omega_s$ , if and only if  $\rho' = \rho \otimes \omega_{s-s'}$ , in which case  $\omega_{s-s'}$  is necessarily of finite order, i.e.  $s - s'$  is a rational multiple of  $2\pi i / \log(Np_K)$ . That being so, we define for irreducible  $\phi = \rho \otimes \omega_s$ :

$$(*) \quad W(\phi) = W(\rho \otimes \omega_s) = (N\mathcal{D}(\rho))^{-s} W(\rho),$$

as suggested by Corollary 5 (i) above. By that Corollary it is obvious that this definition is valid, i.e. independent of the decomposition  $\phi = \rho \otimes \omega_s$ . Having defined  $W(\phi)$  for irreducible  $\phi$ , one extends it to all  $\phi$  by linearity. Since  $\mathcal{D}(\rho_1 + \rho_2) = \mathcal{D}(\rho_1)\mathcal{D}(\rho_2)$ , the formula (\*) holds then for all  $\phi$ , irreducible or not.

We now want to check that the relation:

$$W(\text{Ind}_{L/K} \phi) = \lambda^{\dim(\phi)} W(\phi)$$

holds for all representations  $\phi$  of the Weil group of  $L$ , where  $\lambda = \lambda_{L/K}$  is the constant, which we know exists, such that this equation holds whenever  $\phi$  is a representation of the Galois group. Clearly it is enough to do this for irreducible  $\phi$ , say for  $\phi = \rho \otimes \omega_s$  as above. We have in that case:

$$\text{Ind}_{L/K} \phi = \text{Ind}_{L/K}(\rho \otimes \omega_s) = \text{Ind}_{L/K}(\rho) \otimes \omega_s,$$

because " $\omega_s$  for  $L$ " is the restriction of " $\omega_s$  for  $K$ ". Hence:

$$\frac{W(\text{Ind } \phi)}{W(\phi)} = \frac{W(\text{Ind } \rho)}{W(\rho)} A^{-s} = \lambda^d A^{-s},$$

where  $d = \dim(\phi) = \dim(\rho)$ , and

$$A = \frac{N\mathcal{D}(\text{Ind } \rho)}{N\mathcal{D}(\rho)}.$$

It follows from the theory of the Artin Conductor that  $A = 1$ ; but one can also argue that  $A = 1$  because  $A^{-s} = 1$  whenever  $s$  is a rational multiple of  $2\pi i / \log(N\rho_K)$ . Indeed for such  $s$ , the representation  $\phi = \rho \otimes \omega_s$  comes from the Galois group.

### §3. Root Numbers of Orthogonal Representations

Let  $E/K$  be a finite Galois extension of local or global fields of characteristic 0,  $G = \text{Gal}(E/K)$ , and let

$\rho: G \rightarrow \text{GL}_n(\mathbb{C})$  be a representation. Define:

$$c(\rho) = W(\rho)/W(\det_\rho).$$

#### Proposition 2

- (i) If  $\dim(\rho) = 1$ , then  $c(\rho) = 1$ .
- (ii)  $c(\rho_1 + \rho_2)$   
 $= c(\rho_1)c(\rho_2)W(\det_{\rho_1})W(\det_{\rho_2}).W(\det_{\rho_1}.\det_{\rho_2})^{-1}.$
- (iii)  $c(\rho + \bar{\rho}) = \det_\rho(-1).$
- (iv)  $c(\bar{\rho}) = \overline{c(\rho)}$ , and  $|c(\rho)| = 1.$
- (v) Suppose  $\rho = \bar{\rho}$ . Then  $c(\rho) = \pm 1.$

Proof (i) and (ii) are clear. (iii) is immediate from Theorem 1 Corollary 1 (ii). (iv) follows from Theorem 1 Corollary 1 (i), (ii), and (v) follows from (iv).

We shall be interested in  $c(\rho)$  only when  $\rho$  is an orthogonal representation;  $\rho \in R_G^{\text{IR}}$ , to use the notation of [Dur.M].

Assume that  $K$  is local non-Archimedean, and that  $G$  is a dihedral group. Then  $E \supset L \supset K$ , where  $E/L$  is cyclic,  $L/K$  is quadratic, and each element of  $\text{Gal}(E/K) - \text{Gal}(E/L)$  is of order 2. Take  $\rho = \text{Ind}_{L/K}(\chi)$ , for some 1-dimensional representation  $\chi$  of  $\text{Gal}(E/L)$ . The character  $\det_\rho$  is the non-trivial character of  $\text{Gal}(L/K)$ . The transfer map  $\text{ver}_{L/K}: \text{Gal}(E/K) \rightarrow \text{Gal}(E/L)$  is trivial. So the character  $\chi|K^\times$  of  $K^\times$ , corresponding to  $\chi \circ \text{ver}_{L/K}$  by the local transfer theorem ([Dur.M,3.1]), is also trivial. We may write  $L = K(\delta)$ , for some  $\delta$  such that  $\delta^2 \in K^\times$ . Then  $\text{Tr}_{L/K}(\delta) = 0$ . Also,  $\chi(\delta) = \pm 1$ , and this value is independent of the choice of  $\delta$ .

Theorem 2 (Fröhlich-Quayrut, [FQ]) In the above situation:

$$c(\rho) = \chi(\delta).$$

One verifies easily that  $c(\rho) = W(\chi)$ . We deduce

Theorem 2 from the more general:

Theorem 2' Let  $L/K$  be a finite extension of non-Archimedean local fields, and let  $\chi$  be a character of  $L^\times$  of finite order such that  $\chi|_{K^\times}$  is trivial. Then:

$$W(\chi) = \sum_i \lambda_i \bar{\chi}(\delta_i)$$

for some positive real numbers  $\lambda_i$  and some  $\delta_i \in L^\times$  such that  $\text{Tr}_{L/K}(\delta_i) = 0$ .

To obtain Theorem 2 from Theorem 2', observe that when  $L/K$  is quadratic, the element  $\delta$  such that  $\text{Tr}_{L/K}(\delta) = 0$  is uniquely determined modulo factors from  $K$ . Hence the expression for  $W(\chi)$  in Theorem 2' reduces to  $W(\chi) = \lambda\chi(\delta)$ . Since  $W(\chi)$  and  $\chi(\delta)$  both have absolute value 1, we conclude that  $\lambda = 1$ , and  $W(\chi) = \chi(\delta)$ .

Proof of Theorem 2' Suppose first that  $\chi$  is non-ramified.

Let  $\mathfrak{o}_L = \mathfrak{o}_K[\alpha]$ , and let  $f(X) \in \mathfrak{o}_K[X]$  be the monic

minimal polynomial of  $\alpha$  over  $K$ . Then  $\text{Tr}_{L/K}(f'(\alpha)^{-1}) = 0$ , and  $f'(\alpha)o_L = \mathcal{D}_{L/K}$ . So:

$$W(\chi) = \chi(\mathcal{D}_L) = \chi(\mathcal{D}_{L/K}) = \bar{\chi}(f'(\alpha)^{-1}).$$

Now assume that  $\chi$  is ramified, and let  $b \in L^\times$  be such that  $b o_L = \mathcal{D}(\chi)$ .

Lemma If  $y \in p_L$ ,  $y \neq 0$ , then:

$$\sum_{\substack{x \in o_L^\times \\ \text{mod } \mathfrak{f}(\chi)}} \bar{\chi}(b^{-1}xy) \psi_L(b^{-1}xy) = 0.$$

Proof Observe that the sum in the statement is independent of the choice of representatives  $x$  of  $o_L^\times \text{ mod } \mathfrak{f}(\chi)$ . Let  $\mathfrak{f}(\chi) = p_L a$ , for an ideal  $a$  of  $o_L$ . Then:

$$\begin{aligned} & \sum_{\substack{x \in o_L^\times \\ \text{mod } \mathfrak{f}(\chi)}} \bar{\chi}(b^{-1}xy) \psi_L(b^{-1}xy) \\ &= \sum_{\substack{x \in o_L^\times \\ \text{mod } a}} \bar{\chi}(b^{-1}xy) \sum_{\substack{z \in (1+a) \\ \text{mod } \mathfrak{f}(\chi)}} \bar{\chi}(z) \psi_L(b^{-1}xyz). \end{aligned}$$

The map  $z \mapsto \psi_L(b^{-1}xyz)$  is constant on  $1 + a$  since  $b^{-1}xya \subset \mathcal{O}_L^{-1}$ . But  $\chi$  is a non-trivial character of the group  $(1 + a)/(1 + \mathfrak{f}(\chi))$ , so the inner sum is zero. This proves the Lemma.

For non-zero complex numbers  $a$  and  $b$ , we write  $a \sim b$  if  $ab^{-1}$  is real and positive. Now:

$$W(\chi) \sim \sum_{\substack{x \in \mathcal{O}_L^\times \\ \text{mod } \mathfrak{f}(\chi)}} \bar{\chi}(b^{-1}x) \psi_L(b^{-1}x)$$

hence by the Lemma:

$$W(\chi) \sim \int_{\mathcal{O}_K - \{0\}} \sum_x \bar{\chi}(b^{-1}xy) \psi_L(b^{-1}xy) dy$$

for any Haar measure  $dy$  of  $K^+$ . Since  $\chi$  is trivial on  $K^\times$ , this integral is equal to:

$$\begin{aligned} & \sum_x \bar{\chi}(b^{-1}x) \int_{\mathcal{O}_K} \psi_L(b^{-1}xy) dy \\ &= \sum_x \bar{\chi}(b^{-1}x) \int_{\mathcal{O}_K} \psi_K(y \cdot \text{Tr}_{L/K}(b^{-1}x)) dy \\ &= \sum_{\substack{x \in \mathcal{O}_L^\times \\ \text{mod } \mathfrak{f}(\chi), \\ \text{Tr}_{L/K}(b^{-1}x) \in \mathcal{O}_K^{-1}}} \bar{\chi}(b^{-1}x) \int_{\mathcal{O}_K} \psi_K(y \cdot \text{Tr}_{L/K}(b^{-1}x)) dy, \end{aligned}$$



since the integral is zero if  $\text{Tr}_{L/K}(b^{-1}x) \notin \mathcal{D}_K^{-1}$ . Otherwise, the integral is a positive real number  $\lambda_x$ , say. But  $\text{Tr}_{L/K}(b^{-1}x) \in \mathcal{D}_K^{-1}$  if and only if  $b^{-1}x = d_x + \delta_x$  for some  $d_x \in \mathcal{D}_L^{-1}$  and some  $\delta_x \in L^\times$  with  $\text{Tr}_{L/K}(\delta_x) = 0$ . But  $bd_x \in \mathfrak{f}(\chi)$ , so:

$$\chi(b^{-1}x) = \chi(b^{-1}x - d_x) = \chi(\delta_x),$$

and:

$$W(\chi) \sim \sum_x \lambda_x \bar{\chi}(\delta_x),$$

as asserted.

Corollary 1 (Fröhlich-Queyrut, [FQ]) If  $E/K$  is a finite Galois extension of algebraic number fields, and  $\rho$  is an orthogonal representation of  $\text{Gal}(E/K)$ , then:

$$W(\rho) = 1.$$

Proof The global root number is invariant under induction for virtual representations of arbitrary dimension ("strong extendibility"). The induction theorem for orthogonal representations ([Dur.M, §3]) reduces us to the case in which  $\rho$  is a representation of one of the following three sorts:

$$\rho: \text{Gal}(E/K) \rightarrow \text{GL}_n(\mathbb{C})$$

(i)  $\dim(\rho) = 1$ :

Here,  $\rho$  is either  $[1_K]$ , or the non-trivial character of  $\text{Gal}(L/K)$  with  $L/K$  quadratic, in which case

$$\rho = \text{Ind}_{L/K} [1_L] - [1_K]. \quad \text{In both cases, } W(\rho) = 1.$$

(ii)  $\rho = \theta + \bar{\theta}$ , for some representation  $\theta$ :

$$\text{Here we have } W(\bar{\theta}) = \overline{W(\theta)}, \text{ so } W(\rho) = W(\theta)\overline{W(\theta)} = 1.$$

(iii)  $\rho$  is dihedral:

That is,  $\text{Gal}(E/K)$  is dihedral,  $L/K$  is quadratic,  $E/L$  is cyclic, and  $\rho = \text{Ind}_{L/K}(\chi)$  for some 1-dimensional representation  $\chi$  of  $\text{Gal}(E/L)$ ; in short, the situation is the global analogue of that in Theorem 2.

By the global transfer theorem, [Dur.M,3.1], as idele class character, we have  $\chi|_{C_K} = 1$ . Let  $L = K(\delta)$ , with  $\delta^2 \in K^\times$ .

We already know, by (i), that  $W(\det_\rho) = 1$ . Hence we are reduced to proving  $c(\rho) = 1$ . This will follow if we can show, for each place  $v$  of  $K$ , that:

$$(*) \quad c(\rho_v) = \prod_{w|v} \chi_w(\delta),$$

for then

$$c(\rho) = \prod_v c(\rho_v) = \prod_v \prod_{w|v} \chi_w(\delta) = \prod_w \chi_w(\delta) = \chi(\delta) = 1,$$

because  $\delta \in L^\times$  and  $\chi$  is an idele class character.

If  $v$  is non-Archimedean and undecomposed in  $L$ , then (\*) follows from Theorem 2.

If  $v$  is Archimedean, and undecomposed in  $L$ , then  $L_w$  is complex, hence  $\chi_w = 1$ . On the other hand,  $\rho_v = [1] + \text{sgn}$ , hence  $c(\rho_v) = 1$ , by Proposition 2 (i) and (ii).

Suppose  $v$  splits in  $L$ . Then the decomposition group of  $w|v$  is contained in  $\text{Gal}(E/L)$ , so  $\rho_v = \chi_w + \bar{\chi}_w$  and by Proposition 2 (ii) we have:

$$c(\rho_v) = c(\chi_w + \bar{\chi}_w) = \chi_w(-1).$$

On the other hand, if  $w'$  is the other place of  $L$  above  $v$ , then:

$$\chi_w(\delta)\chi_{w'}(\delta) = \chi_w(-1),$$

because  $\chi_{w'}(\delta) = \bar{\chi}_w(-\delta)$ . Hence (\*) holds in every case.

Let  $(a,b)_K$  denote the quadratic norm-residue ("Hilbert") symbol for the local field  $K$  ([CF,p.351]), and let  $\chi_a(x) = (a,x)_K$  denote the quadratic character corresponding to the extension  $K(\sqrt{a})/K$ .

Corollary 2 For  $a$  and  $b$  in  $K^\times$  we have:

$$W(\chi_a)W(\chi_b) = W(\chi_{ab}) \cdot (a,b)_K.$$

Proof If  $\chi_{ab} = 1$ , i.e.  $\chi_a = \chi_b$ , the formula to be proved boils down to  $(W(\chi_a))^2 = (a, a)_K = (a, -1)_K = \chi_a(-1)$ , which is true by Corollary 1 (ii) of Theorem 1. Suppose  $\chi_{ab} \neq 1$ . Then we can apply Theorem 2 to the situation:

$$E = K(\sqrt{a}, \sqrt{b}), \quad L = K(\sqrt{ab}), \quad \delta = \sqrt{ab}$$

$$\chi = \chi_a \text{ (on } L^\times), \quad \rho = \chi_a + \chi_b, \quad \text{and let } \det_\rho = \chi_{ab}.$$

We find:

$$W(\chi_a)W(\chi_b)W(\chi_{ab})^{-1} = c(\rho) = (a, \sqrt{ab})_L.$$

This proves the Corollary because:

$$(a, \sqrt{ab})_L = (a, N_{L/K}(\sqrt{ab}))_K = (a, -ab)_K = (a, b)_K.$$

We can define the Hilbert symbol on real characters of  $K^\times$  by setting:

$$(\chi_a, \chi_b)_K = (a, b)_K.$$

Using this and Corollary 2, we see that Proposition 2 (ii) can be rewritten as:

$$(**) \quad c(\rho_1 + \rho_2) = c(\rho_1)c(\rho_2) \cdot (\det_{\rho_1}, \det_{\rho_2}).$$

Deligne in [D0] gives an alternative interpretation of  $c(\rho)$  for an orthogonal representation in the local case. This gives a local explanation of the global Corollary 1.

If  $G$  is any finite group, and:

$$\rho: G \rightarrow O(n)$$

is an orthogonal representation of  $G$ , we denote the  $i$ -th Stiefel-Whitney invariant of  $\rho$  by:

$$\delta_i(\rho) \in H^i(G, \mathbb{Z}/2\mathbb{Z}).$$

In low dimensions  $i$ , the Stiefel-Whitney invariant is given algebraically as follows. Under the canonical isomorphism:

$$H^1(G, \mathbb{Z}/2\mathbb{Z}) \simeq \text{Hom}(G, \{\pm 1\}),$$

the image of  $\delta_1(\rho)$  is  $\det_\rho$ . If  $\delta_1(\rho)$  is trivial, i.e.

$\det_\rho = 1$ , then  $\delta_2(\rho)$  is the element of  $H^2(G, \{\pm 1\}) = H^2(G, \mathbb{Z}/2\mathbb{Z})$  which is the inverse image under  $\rho: G \rightarrow SO(n)$  of the class of the extension:

$$1 \rightarrow \{\pm 1\} \rightarrow \text{Spin}(n) \rightarrow SO(n) \rightarrow 1,$$

where  $SO$  denotes the special orthogonal group and  $\text{Spin}$  the spinor group.

Now take  $G = \text{Gal}(E/K)$ , for some finite extension  $E/K$  of local fields. Then:

$$H^2(G, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\text{inf}} H^2(\Omega_K, \mathbb{Z}/2\mathbb{Z}) = \text{Br}(K)_2 \simeq \{\pm 1\} \quad (K \neq \mathbb{C}),$$

where  $\text{inf.}$  denotes inflation (which is injective), and

$\text{Br}(K)_2$  denotes the 2-part of the Brauer group of  $K$ . Write

$\text{cl}(\delta_2(\rho))$  for the image of  $\delta_2(\rho)$  in  $\{\pm 1\}$  under the

composition of these maps. Then:

Theorem 3 (Deligne) Let  $E/K$  be a finite Galois extension of local fields, and let  $\rho$  be an orthogonal representation of  $\text{Gal}(E/K)$ . Then:

$$\text{cl}(\mathcal{S}_2(\rho)) = c(\rho)$$

Let  $R^0(K)$  be the set of pairs  $(L, \rho) \in R(K)$  such that  $\rho$  is an orthogonal representation of  $\Omega_L$ . By an induction theorem for orthogonal representations similar to the one proved in [Dur.M, §3], one can prove that the function  $c: R^0(K) \rightarrow \{\pm 1\}$  is the unique function satisfying the following three conditions:

(a) Proposition 2 (i), Proposition 2 (iii), and Theorem 2 (these give the values of  $c$  on the three basic types of orthogonal representation).

(b) Proposition 2 (ii) (the addition rule for  $c$ ).

(c) If  $K \subset L' \subset L$  and  $(L, \rho) \in R^0(K)$  satisfies  $\dim(\rho) = 0$  and  $\det_\rho = 1$ , then  $c(\text{Ind}_{L/L'}(\rho)) = c(\rho)$  (induction rule).

Deligne shows that the function  $\rho \mapsto \text{cl}(\mathcal{S}_2(\rho))$  satisfies these three conditions and is therefore equal to  $c(\rho)$ . For details, see [D0]. We note that condition (b), in the form (\*\*) above, corresponds to the rule:

$$\delta_2(\rho_1 + \rho_2) = \delta_2(\rho_1) + \delta_2(\rho_2) + \delta_1(\rho_1) \cup \delta_1(\rho_2) \quad ,$$

( $\cup$  means cup-product) in virtue of the fact that  $\delta_1(\rho) = \det_\rho$ , and that, with suitable interpretations,  $(\chi_1, \chi_2) = \chi_1 \cup \chi_2$  (cf. [CL, Ch. XIV, §2, Prop. 5]).

The global Fröhlich-Queyrut theorem, Corollary 1 of Theorem 2, is an immediate consequence of Theorem 3. Let  $E/K$  be a finite Galois extension of algebraic number fields, and let  $\rho$  be an orthogonal representation of  $\text{Gal}(E/K)$ . If  $v$  is any place of  $K$ , then  $\delta_2(\rho_v)$  is the image of  $\delta_2(\rho)$  under the canonical localisation (restriction) map:

$$H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(G_v, \mathbb{Z}/2\mathbb{Z}) \quad ,$$

where  $G = \text{Gal}(E/K)$ , and  $G_v$  is a decomposition group of  $v$ . Thus the elements  $\text{cl}(\delta_2(\rho_v)) = c(\rho_v)$  are the local invariants of an element (of order dividing 2) in the global Brauer group. Therefore  $c(\rho)$ , the product of these invariants, is indeed 1.

## REFERENCES

This volume:

[Dur.M] J. Martinet, Character theory and Artin L-functions.



Others:

- [AT] E. Artin & J. Tate, Class Field Theory (Benjamin, New York, 1967).
- [CF] J.W.S. Cassels & A. Fröhlich, Algebraic Number Theory (Academic Press, London, 1967).
- [CL] J-P.Serre, Corps Locaux (Hermann, Paris, 1962).
- [D] P. Deligne, Les constantes des équations fonctionnelles des fonctions L (Springer Lecture Notes 349 (1974) pp. 501-597).
- [DO] P. Deligne, Les constantes locales de l'équation fonctionnelle de la fonction L d'Artin d'une représentation orthogonale (to appear in Inv. Math.)
- [Dw] B. Dwork, On the Artin root number (Amer. J. Math. 78, 1956, 444-472).
- [FQ] A. Fröhlich & J. Queyrut, On the functional equation of the Artin L-function for characters of real representations (Inv. Math. 14, 1971, 173-183).
- [L] R.P. Langlands, On Artin's L-functions, in Complex Analysis (Rice University Studies 56, 1970, 23-28).
- [S] J-P. Serre, Représentations Linéaires des Groupes Finis (Hermann, Paris, 1971 (2nd. ed.)).
- [T] J.T. Tate, Fourier analysis in number fields and Hecke's zeta-functions (thesis, Princeton University 1950; published in [CF], 305-347).
- [W] A. Weil, Basic Number Theory (Springer-Verlag, Berlin, 1974 (2nd. ed.)).



## Galois module structure

A. Fröhlich

The central topic of these notes is the global structure of the ring of algebraic integers in a normal extension  $N/K$  of number fields, as a module over the Galois group. Compared to the original notes, distributed in Durham, the presentation here has been expanded and recast, although covering essentially the same material. Some new ideas and results have been incorporated, in particular the notion of an adelic resolvent. We also give a new treatment of properties on change of base field or of group; the connection between norms of homomorphisms and restriction of scalars has now been clarified.

The notes have been subdivided into three main parts. The first part is concerned principally with the theorems on Galois module structure, the second with the underlying resolvent theory, and the third part - which may be read independently of part II and which may be viewed as a

supplement to Martinet's lectures (cf. [M3]) - deals with root numbers and Galois Gauss sums. We mostly give only brief outlines of proofs. In the nature of things these are mainly contained in Parts II and III. There is an appendix, which deals with some of the subject matter of Part II in a more formal manner.

Notations. As usual,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  are the ring of integers and the field of rational, of real, and of complex numbers, respectively. The multiplicative group of a ring  $S$  is denoted by  $S^*$ . The Galois group of a normal field extension  $E/F$  is  $\text{Gal}(E/F)$ . The algebraic closure of  $\mathbb{Q}$  in  $\mathbb{C}$  is denoted by  $\bar{\mathbb{Q}}$  and a "number field"  $K$  is always a subfield of  $\bar{\mathbb{Q}}$  of finite degree over  $\mathbb{Q}$ . We then write  $\text{Gal}(\bar{\mathbb{Q}}/K) = \Omega_K$ . The symbol  $\mathcal{O}_K$ , or just  $\mathcal{O}$ , stands for the ring of algebraic integers in  $K$ . Completions at prime divisors of  $K$  are indicated by appropriate subscripts, with the convention that if  $\mathfrak{p}$  is an infinite prime divisor and  $M$  an  $\mathcal{O}$ -lattice then  $M_{\mathfrak{p}}$  is actually the completion of  $MK$ . We shall often consider completions with respect to prime divisors of subfields (semi-local completions), denoted in the same way.

Part I. Theorems on Galois module structure§1. Background

Throughout  $\Gamma$  is a finite group and  $K$  a number field.

Assume we are given a surjective homomorphism

$$(1.1) \quad \pi: \Omega_K \rightarrow \Gamma'$$

with open kernel and we denote by  $N$  the fixed field of  $\text{Ker } \pi$ .

Then we have an isomorphism

$$(1.2) \quad \tilde{\pi}: \Gamma \cong \text{Gal}(N/K),$$

which we use to make  $N$ ,  $\mathcal{O}_N$  etc. into  $\Gamma$ -modules. (Except in §14,  $\pi$  is really fixed and need not be referred to). We wish specifically to study  $\mathcal{O}_N = 0$  (notation used throughout) as a module over the group ring  $\mathcal{O}(\Gamma)$  (of  $\Gamma$  over  $\mathcal{O} = \mathcal{O}_K$ ) or more generally over  $\mathcal{O}_k(\Gamma)$ , where  $k$  is a subfield of  $K$ , and in particular over  $\mathbb{Z}(\Gamma)$ .

The first attack is via localisation. Let  $M$  be an  $\mathcal{O}_k(\Gamma)$ -module, which is an  $\mathcal{O}_k$ -lattice, i.e. is finitely generated and torsion free over  $\mathcal{O}_k$ . We shall say that  $M$  is locally free (of rank  $n$ ) over  $\mathcal{O}_k(\Gamma)$ , if for all prime divisors  $p$  of  $k$ , the  $\mathcal{O}_{k,p}(\Gamma)$ -module  $M_p$  is free of rank  $n$ . We know, essentially by a theorem of E. Noether, that the following conditions on  $\mathcal{O}$  are equivalent: (i)  $\mathcal{O}$  is locally

free over  $\mathcal{O}(\Gamma)$ , (ii) for some  $k \subset K$ ,  $\mathcal{O}$  is locally free over  $\mathcal{O}_k(\Gamma)$ , (iii) the extension  $N/K$  is tame (at most tamely ramified). Moreover if  $\mathcal{O}$  is locally free then its rank over  $\mathcal{O}_k(\Gamma)$  is the degree  $[K:k]$ . We shall assume this to be the case and then study the global Galois module structure of  $\mathcal{O}$ . This turns out to be closely connected with arithmetic character invariants and in particular with the constants in the functional equation of the Artin L-function. For other brief reports see [M2], [F8], [F9] and for a detailed exposition see [F10], where most of the required details can be found. For resolvent theory see also [F1] and [F7].

## §2. The classgroup of a group ring

The definitions and results of this section apply to any triplet  $(\Gamma, K, \mathcal{O})$  where  $\Gamma$  is a finite group,  $K$  a number field,  $\mathcal{O}$  its ring of integers. The representation of  $\Gamma$  as Galois group (cf. (1.1), (1.2)) is not used here and is irrelevant.

Throughout these notes  $E$  is an absolutely normal number field which is "big enough". In general terms this means that for various functors  $G$  of number fields which we shall

have to consider, the maps  $G(E) \rightarrow G(E')$  induced by embeddings  $E \subset E'$  become isomorphisms. (As an alternative we could have replaced  $E$  by  $\bar{\mathbb{Q}}$  and defined the objects  $G(\bar{\mathbb{Q}})$  as limits).

Effectively what we need is that  $E$  contains  $K$  (and subsequently also some normal extension  $N$  of  $K$ ), and the values of all characters of  $\Gamma$ , in the sense of representation theory. It will be convenient also to assume that each character of  $\Gamma$  actually corresponds to a matrix representation of  $\Gamma$  over  $E$ .

Let  $R_\Gamma$  be the additive group of virtual characters of  $\Gamma$ , i.e., the free Abelian group on the (absolutely) irreducible characters.  $\Omega_{\mathbb{Q}}$  acts on  $R_\Gamma$ , e.g., by viewing the virtual characters as functions  $\Gamma \rightarrow \bar{\mathbb{Q}}$ . Thus for  $\chi \in R_\Gamma$ ,  $\omega \in \Omega_{\mathbb{Q}}$ ,  $\gamma \in \Gamma$ , we have  $\chi^\omega(\gamma) = \chi(\gamma)^\omega$ . Moreover  $\Omega_K$  acts on the multiplicative group  $E^*$  of  $E$  and on its idele group  $J(E)$ . We thus get a group  $\text{Hom}_{\Omega_K}(R_\Gamma, J(E))$  with subgroup  $\text{Hom}_{\Omega_K}(R_\Gamma, E^*)$ . Next let  $U(o(\Gamma))$  be the group of unit ideles of  $o(\Gamma)$ , i.e., the product over all prime divisors  $p$  of  $K$  of the groups  $o_p(\Gamma)^*$ . Let  $\chi$  be a character of  $\Gamma$ , corresponding to a representation  $T: \Gamma \rightarrow \text{GL}(n, \bar{\mathbb{Q}})$ . We extend  $T$  to an algebra homomorphism  $K(\Gamma) \rightarrow M_n(\bar{\mathbb{Q}})$  ( $n$  by  $n$  matrices over  $\bar{\mathbb{Q}}$ ), and define for  $\lambda \in K(\Gamma)$ ,

$$\text{Det}_\chi(\lambda) = \text{Det } T(\lambda).$$



Then  $\text{Det}_\chi(\lambda) \in E^*$  for  $\lambda \in K(\Gamma)^*$ . We can extend  $\text{Det}_\chi$  further to a function on ideles of  $K(\Gamma)$ , and so in particular  $\text{Det}_\chi(\lambda)$  is defined for  $\lambda \in U(\mathcal{O}(\Gamma))$  and has values in  $J(E)$ . Finally if  $\chi, \psi$  are characters, we put  $\text{Det}_{\chi\psi}(\lambda) = \text{Det}_\chi(\lambda) \cdot \text{Det}_\psi(\lambda)^{-1}$ . Thus  $\text{Det}_\chi$  is defined for  $\chi \in R_\Gamma$ . Now let  $\mu \in U(\mathcal{O}(\Gamma))$ . Then the map  $\text{Det}(\mu) : \chi \mapsto \text{Det}_\chi(\mu)$  is an  $\Omega_K$ -homomorphism  $R_\Gamma \rightarrow J(E)$ . The map  $\text{Det} : U(\mathcal{O}(\Gamma)) \rightarrow \text{Hom}_{\Omega_K}(R_\Gamma, J(E))$  which takes  $\mu$  into  $\text{Det}(\mu)$  is a homomorphism. We define the class group by

$$(2.1) \quad \text{Cl}(\mathcal{O}(\Gamma)) = \text{Hom}_{\Omega_K}(R_\Gamma, J(E)) / \text{Hom}_{\Omega_K}(R_\Gamma, E^*) \cdot \text{Det } U(\mathcal{O}(\Gamma)).$$

Remark It is clear that the choice of  $E$  within the stated conditions is immaterial.

Let  $J(E, \Gamma)$  be the subgroup of ideles, whose semilocal components at all rational prime divisors  $p$  of order  $(\Gamma)$  and at  $p = \infty$  are  $= 1$ . The map  $J(E, \Gamma) \rightarrow J(E)$  yields a surjective homomorphism of  $\text{Hom}_{\Omega_K}(R_\Gamma, J(E, \Gamma))$  onto  $\text{Cl}(\mathcal{O}(\Gamma))$ , and if  $U(E, \Gamma)$  denotes the subgroup of  $J(E, \Gamma)$  of ideles with unit components everywhere, then  $\text{Hom}_{\Omega_K}(R_\Gamma, U(E, \Gamma)) \subset \text{Det } U(\mathcal{O}(\Gamma))$ . On the other hand associate with each  $f \in \text{Hom}_{\Omega_K}(R_\Gamma, J(E, \Gamma))$

the function  $b_f$ , with  $b_f(\chi)$  the fractional ideal  $(f(\chi))$  generated by  $f(\chi)$  (the contents of  $f(\chi)$ ). We then obtain an isomorphism

$$\text{Hom}_{\Omega_K}(R_\Gamma, J(F, E)) / \text{Hom}_{\Omega_K}(R_\Gamma, U(\Gamma, E)) \cong I_{O, \Gamma},$$

where  $I_{O, \Gamma}$  is the group of maps  $b$  from  $R_\Gamma$  to fractional ideals of  $O_E$  (the ring of algebraic integers in  $E$ ) with the following properties:

- (i)  $b(\chi)$  has numerator and denominator prime to order  $(\Gamma)$ .
- (ii)  $b(\chi)$  is actually a fractional ideal of  $O_{K(\chi)}$ , where  $K(\chi)$  always denotes the field obtained by adjoining to  $K$  the values of  $\chi$  and  $O_{K(\chi)}$  is its ring of algebraic integers.
- (iii) For  $\omega \in \Omega_K$ ,  $b(\chi^\omega) = b(\chi)^\omega$ .

Putting everything together one gets a surjection

$I_{O, \Gamma} \rightarrow \text{Cl}(O(\Gamma))$ . One can determine its kernel  $H_{O, \Gamma}$ . It is the subgroup of  $I_{O, \Gamma}$  for which  $b(\chi) = (b(\chi))$ , with  $b \in \text{Hom}_{\Omega_K}(R_\Gamma, E^*)$  and so that for all rational primes  $p$  dividing order  $(\Gamma)$  and for  $p = \infty$  we have, in the obvious notation,  $b_p \in \text{Det } O_p(\Gamma)^*$ , where the subscripts  $p$  denote completion at semilocal components. Thus we get an isomorphism

$$(2.2) \quad I_{\mathcal{O}, \Gamma} / H_{\mathcal{O}, \Gamma} \stackrel{\sim}{=} \text{Cl}(\mathcal{O}(\Gamma)) \quad .$$

Remark We shall not prove that our class group is the usual one, but we shall show how one associates with a locally free rank 1 module  $M$  an element  $(M)$  of  $\text{CL}(\mathcal{O}(\Gamma))$ . One can then prove that every element of  $\text{Cl}(\mathcal{O}(\Gamma))$  is of form  $(M)$ , that  $(M) = (N)$  precisely when  $M$  and  $N$  are stably isomorphic, that for many groups  $(M) = (N)$  implies  $M \cong N$ , and that  $(\mathcal{O}(\Gamma))$  is the unit element.

The  $K$ -vector space  $V$  spanned by  $M$  has the structure of a  $K(\Gamma)$ -module, and in fact is free of rank 1 over  $K(\Gamma)$ . Let  $V = v K(\Gamma)$ . Then for some idele  $\beta$  of  $K(\Gamma)$ , we have  $M = v\beta\mathcal{O}(\Gamma)$ , this to be understood as a set of equations  $M_p = v\beta_p \mathcal{O}_p(\Gamma)$ . Define  $f(\chi) = \text{Det}_{\chi}(\beta)$ . Then  $f \in \text{Hom}_{\Omega_K}(R_{\Gamma}, J(E))$  and the class  $(M)$  of  $f$  in  $\text{Cl}(\mathcal{O}(\Gamma))$  indeed is independent of arbitrary choices and only depends on the isomorphism class of  $M$ . One may moreover choose  $v$  above so that  $M_p = v \mathcal{O}_p(\Gamma)$  for all  $p \mid \text{order}(\Gamma)$ . Then the equations  $b(\chi) = (\text{Det}_{\chi}(\beta))$  define an element in  $I_{\mathcal{O}, \Gamma} / H_{\mathcal{O}, \Gamma}$  corresponding to  $(M)$ . We shall call  $\{b(\chi)\}$  a family of invariants for  $M$ .

Remark For rank  $> 1$  one proceeds analogously. Only now one has to extend the homomorphism  $T: K(\Gamma) \rightarrow M_n(\bar{\mathbb{Q}})$  to one  $M_m(K(\Gamma)) \rightarrow M_{mn}(\bar{\mathbb{Q}})$ , and analogously for adeles.

Let  $U(E)$  be the group of unit ideles of  $E$ , i.e., of ideles which are units at all finite places. Different from the usual terminology, we shall call an idele  $\alpha$  of  $E$  totally positive if  $\alpha_p$  is real and positive for all infinite prime divisors  $p$ , including the complex ones. We call a character  $\chi$  of  $\Gamma$  symplectic if it is the character of a symplectic representation, and we write  $R_\Gamma^S$  for the subgroup of  $R_\Gamma$  generated by the symplectic characters. Any virtual character  $\chi \in R_\Gamma^S$  will then also be called symplectic. We write  $\text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_\Gamma, U(E))$  for the subgroup of  $\text{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E))$  of maps  $f$  with  $f(\chi)$  totally positive whenever  $\chi$  is symplectic. This group contains  $\text{Det } U(\mathbb{Z}(\Gamma))$ . Thus one has a surjection

$$(2.3) \quad \text{Cl}(\mathbb{Z}(\Gamma)) \rightarrow \text{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma, J(E)) / \text{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma, E^*) \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_\Gamma, U(E)),$$

whose kernel we denote by  $D(\mathbb{Z}(\Gamma))$  (the so called kernel group of  $\mathbb{Z}(\Gamma)$ ). In fact the group on the right in (2.3) may be viewed as the class group  $\text{Cl}(M)$ , where  $M$  is any maximal order of  $\mathbb{Q}(\Gamma)$ , and the map (2.3) as given by

extension of scalars to  $M$  (containing  $Z(\Gamma)$ ). We clearly have an isomorphism

$$(2.4) \quad D(Z(\Gamma)) \stackrel{\sim}{=} \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_{\Gamma}, U(E)) / \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_{\Gamma}, \sigma_E^*) \text{Det } U(Z(\Gamma)),$$

$$\text{where } \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_{\Gamma}, \sigma_E^*) = \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_{\Gamma}, \sigma_E^*) \cap \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_{\Gamma}, U(E)).$$

In terms of families of invariants, the isomorphism (2.2) for  $\sigma = \mathbb{Z}$  yields an isomorphism

$$(2.5) \quad P_{\mathbb{Z}, \Gamma} / H_{\mathbb{Z}, \Gamma} \stackrel{\sim}{=} D(\mathbb{Z}(\Gamma)),$$

where  $P_{\mathbb{Z}, \Gamma}$  is characterised in  $I_{\mathbb{Z}, \Gamma}$  by

$$b(\chi) = (b(\chi)), \quad b \in \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_{\Gamma}, E^*),$$

+ having the obvious meaning, as above.

Let  $k$  be a subfield of  $K$ . As  $\Omega_K \setminus \Omega_k$  is finite we have the usual trace map on homomorphisms, which in view of our multiplicative notation we shall rather call a norm map

$N_{K/k}$ . If  $\{\sigma\}$  is a right transversal of  $\Omega_K$  in  $\Omega_k$  and  $f \in \text{Hom}_{\Omega_K}(R_{\Gamma}, J(E))$  then we define  $N_{K/k} f \in \text{Hom}_{\Omega_k}(R_{\Gamma}, J(E))$  by

$$(2.6) \quad (N_{K/k} f)(\chi) = \prod_{\sigma} f(\chi^{\sigma^{-1}})^{\sigma}.$$

For  $k = \mathbb{Q}$  in particular this induces a norm map

$$(2.7) \quad N_{K/\mathbb{Q}} : \text{Cl}(\mathcal{O}(\Gamma)) \rightarrow \text{Cl}(\mathbb{Z}(\Gamma)).$$

In fact

$$(2.8) \quad N_{K/\mathbb{Q}}((M)_{\mathcal{O}(\Gamma)}) = (M)_{\mathbb{Z}(\Gamma)}.$$

(See (16.5) for further details).

### §3. Resolvents, Galois Gauss sums and Module structure

Here we take  $\Gamma$ ,  $K$  and  $N$  as given in §1. To compute the classes

$$(0)_{\mathcal{O}(\Gamma)} \in \text{Cl}(\mathcal{O}(\Gamma)), \quad (0)_{\mathbb{Z}(\Gamma)} \in \text{Cl}(\mathbb{Z}(\Gamma))$$

one has to generalise the notion of a Lagrange resolvent.

Let  $\chi$  be a character of  $\Gamma$ , corresponding to a representation  $T: \Gamma \rightarrow \text{GL}(n, \bar{\mathbb{Q}})$  and let  $a \in N$  generate a normal basis  $\{a^\gamma\}$  ( $\gamma \in \Gamma$ ) of  $N/K$ . We define the resolvent by

$$(3.1) \quad (a|\chi) = \det\left(\sum_{\gamma} a^\gamma T(\gamma)^{-1}\right).$$

This is a non-zero element of  $\bar{\mathbb{Q}}$ , which only depends on  $a$  and on  $\chi$ . Let  $k \subset K$ . Analogously to (2.6) we define

$$(3.2) \quad N_{K/k}(a|\chi) = \prod_{\sigma} (a|\chi^{\sigma^{-1}})^{\sigma},$$

where  $\{\sigma\}$  is again a right transversal of  $\Omega_K$  in  $\Omega_k$ .

Warning This is not the norm from  $K$  to  $k$  of some element  $x$  of  $K$ . Instead one should view  $N_{K/k}(a|\chi)$  as  $(N_{K/k} f)(\chi)$ , with  $f(\chi) = (a|\chi)$  - except that now the map  $f$  no longer commutes with the operations of  $\Omega_{\mathbb{Q}}$ , or of  $\Omega_K$ , as it did in §1. Moreover  $N_{K/k}(a|\chi)$  still depends on the choice of  $\{\sigma\}$ , but only to within a trivial root of unity factor.

Note that

$$(a|\chi + \psi) = (a|\chi) (a|\psi) ,$$

or more generally

$$N_{K/k}(a|\chi + \psi) = N_{K/k}(a|\chi) N_{K/k}(a|\psi).$$

Thus we may take  $\chi$  to run over all the virtual character.

Let now  $W(\chi)$  be the Artin root number and  $\tau(\chi)$  the Galois Gauss sum, if  $\chi$  is viewed as a character of  $\Omega_K$  via its surjection onto  $\Gamma$  (cf. [M3] 1 and 2, §7 for definitions).

Theorem 1.    The map

$$\chi \mapsto \tau(\chi) N_{K/\mathbb{Q}}(a|\chi)^{-1}$$

lies in

$$\text{Hom}_{\Omega_{\mathbb{Q}}} (R_{\Gamma}, E^*) .$$

Suppose now that  $N/K$  is tame and choose  $a$  so that,  
for all prime divisors  $p$  of order  $(\Gamma)$ , it generates a local



normal integral basis, i.e.,  $0_p = a0_p(\Gamma)$ . Then the fractional ideals

$$b(\chi) = (\tau(\chi) N_{K/\mathbb{Q}} (a|\chi)^{-1})$$

define a family of invariants for  $(0)_{\mathbb{Z}(\Gamma)}$ .

Recall that the subscript  $p$  is completion at the rational prime  $p$ .

Theorem 2. If  $\chi \in R_\Gamma^S$  (i.e.  $\chi$  is symplectic), then  $\tau(\chi) N_{K/\mathbb{Q}} (a|\chi)^{-1}$  is totally real, either totally positive or totally negative, with its sign independent of  $a$  and given by

$$\text{sign}(\tau(\chi) N_{K/\mathbb{Q}} (a|\chi)^{-1}) = W(\chi).$$

From these two theorems, and (2.5) we immediately get the first main theorem of Galois module structure.

Theorem 3 Suppose  $N/K$  is tame. Then

$$(0)_{\mathbb{Z}(\Gamma)} \in D(\mathbb{Z}(\Gamma)) .$$

Thus if  $M$  is a maximal order of  $\mathbb{Q}(\Gamma)$  containing  $\mathbb{Z}(\Gamma)$

then the module  $OM$  is stably free over  $M$ . For  $K = \mathbb{Q}$  this was conjectured by Martinet. (Note that for rank  $> 1$ , i.e., for  $K \neq \mathbb{Q}$ , "stably free" implies "free".)

#### §4. Root numbers and Galois module structure

For the background on representation theory see e.g. [S].

Let  $\ell$  be a prime number and  $R_\Gamma^{(\ell)}$  the Grothendieck group of  $\bar{k}_\ell(\Gamma)$ -modules, where  $\bar{k}_\ell$  is the algebraic closure of the field of  $\ell$ -elements. There is a reduction or "decomposition" map  $d_\ell: R_\Gamma \rightarrow R_\Gamma^{(\ell)}$ , unique to within  $\Omega_{\mathbb{Q}}$ -conjugacy. We are concerned with its kernel  $\text{Ker } d_\ell$  which can also be defined canonically as the set of virtual characters which, when viewed as functions on  $\Gamma$ , vanish on the  $\ell$ -regular elements, i.e., on the elements of order prime to  $\ell$ .

With  $E$  as in §2, let  $L_E$  be the product of prime ideals of  $\mathcal{O}_E$  above  $\ell$  and write

$$W_\ell = (\mathcal{O}_E / L_E)^* \quad (\text{multiplicative group}).$$

If  $f \in \text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma, U(E))$ , then the composition

$$R_\ell(f): \text{Ker } d_\ell \rightarrow R_\Gamma \xrightarrow{f} U(E) \xrightarrow{\text{mod } L_E} W_\ell$$

lies in  $\text{Hom}_{\Omega_{\mathbb{Q}}} (\text{Ker } d_\ell, W_\ell)$ . We thus get a homomorphism

$$(4.1) \quad R_\ell : \text{Hom}_{\Omega_Q}^+(R_\Gamma, U(E)) \rightarrow \text{Hom}_{\Omega_Q}(\text{Ker } d_\ell, W_\ell).$$

For  $\ell \nmid \text{order}(\Gamma)$  of course, the group on the right is null.

A crucial property of  $R_\ell$  is

$$(4.2) \quad \text{Det } U(\mathbb{Z}(\Gamma)) \subset \text{Ker } R_\ell.$$

In fact let  $\theta \in \text{Ker } d_\ell$ . Then  $\theta = \chi - \psi$ , where  $\chi$  and  $\psi$  are actual characters with  $d_\ell(\chi) = d_\ell(\psi)$ . This means that the  $\bar{k}_\ell(\Gamma)$ -modules obtained by reduction mod  $\ell$  from representations of  $\Gamma$ , corresponding to  $\chi$  and to  $\psi$ , have the same composition factors. Hence the determinants in characteristic  $\ell$  coincide, i.e., we have

$$(4.3) \quad \text{Det}_\chi(\lambda) \equiv \text{Det}_\psi(\lambda) \pmod{L_E}$$

for  $\lambda \in \mathbb{Q}(\Gamma)^*$ . This yields (4.2).

Define

$$(4.4) \quad E_\ell(\Gamma) = \text{Hom}_{\Omega_Q}(\text{Ker } d_\ell, W_\ell) / R_\ell(\text{Hom}_{\Omega_Q}^+(R_\Gamma, \sigma_E^*))$$

If  $\ell \nmid \text{order}(\Gamma)$  then of course  $E_\ell(\Gamma) = 0$ . As  $R_\ell$  can be shown to be surjective, and by (2.4), (4.2) we now obtain a surjective homomorphism

$$(4.5) \quad h_\ell : D(\mathbb{Z}(\Gamma)) \rightarrow E_\ell(\Gamma)$$

Next let  $T: R_\Gamma \rightarrow R_\Gamma$  be the map  $T(\phi) = \phi + \bar{\phi}$ , where  $\bar{\phi}$

is the complex conjugate of  $\phi$ . Then  $T(R_\Gamma) \subset R_\Gamma^S$ , and  $R_\Gamma^S/T(R_\Gamma)$  is an  $\Omega_{\mathbb{Q}}$ -module and a vector space over the field with 2 elements. There is then a unique homomorphism  $R_\Gamma \rightarrow R_\Gamma^S/T(R_\Gamma)$  which takes any irreducible symplectic character to its class mod  $T(R_\Gamma)$  and any other irreducible character into zero. We define a homomorphism

$$s_\ell: \text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma^S/T(R_\Gamma), \pm 1) \rightarrow \text{Hom}_{\Omega_{\mathbb{Q}}} (\text{Ker } d_\ell, W_\ell)$$

by taking, for given  $f$ ,  $s_\ell(f)$  as the compositum

$$\text{Ker } d_\ell \rightarrow R_\Gamma \rightarrow R_\Gamma^S/T(R_\Gamma) \xrightarrow{f} \pm 1 \xrightarrow{\text{mod } L_E} W_\ell.$$

Now  $s_\ell$  yields a homomorphism

$$(4.6) \quad k_\ell: \text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma^S/T(R_\Gamma), \pm 1) \rightarrow E_\ell(\Gamma).$$

If now  $N/K$  is tame, then - on viewing  $\chi$  as a character of  $\Omega_K$  via the surjection  $\pi$  of (1.1) - the map  $\chi \mapsto W(\chi) = W(N/K, \chi)$  will lie in  $\text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma^S/T(R_\Gamma), \pm 1)$ , as shown in Martinet's lectures (cf. [M3] 2, Theorem 7.4). We denote this element of  $\text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma^S/T(R_\Gamma), \pm 1)$  by  $W(N/K)$ . (Abuse of notation: It really depends on the choice of  $\pi$  in (1.1), not just on  $N$ . Anyway at this stage it becomes natural to consider not only just one field  $N$ , but all

"tame representations" of  $\Gamma$  over  $K$ . We shall briefly discuss the problem of the range of possible elements  $W(N/K)$  in §14).

Let now  $\ell$  be a prime factor of order  $(\Gamma)$ . (Otherwise we have  $\text{Ker } d_\ell = 0$  and the preceding maps are all null). We get the second main theorem on Galois module structure.

Theorem 4    Suppose that  $N/K$  is tame. Then

$$h_\ell((0)_{\mathbb{Z}(\Gamma)}) = k_\ell(W(N/K)).$$

In particular

$$h_\ell((0)_{\mathbb{Z}(\Gamma)})^2 = 1,$$

and if  $\ell = 2$ , or if  $\Gamma$  has no irreducible symplectic characters, then

$$h_\ell((0)_{\mathbb{Z}(\Gamma)}) = 1.$$

A variant of the last theorem is obtained by restricting to symplectic characters. One gets a map

$$R_\ell^S: \text{Hom}_{\Omega_{\mathbb{Q}}}^+(R_\Gamma, U(E)) \rightarrow \text{Hom}_{\Omega_{\mathbb{Q}}}^S(R_\Gamma^S \cap \text{Ker } d_\ell, W_\ell)$$

yielding a homomorphism

$$(4.7) \quad h^S: D(\mathbb{Z}(\Gamma)) \rightarrow E^S(\Gamma)$$

$$= \prod_{\ell} \text{Hom}_{\Omega_{\mathbb{Q}}} (R_{\Gamma}^S \cap \text{Ker } d_{\ell}, W_{\ell}) / (\prod_{\ell} R_{\ell}^S) (\text{Hom}_{\Omega_{\mathbb{Q}}}^+ (R_{\Gamma}, \mathcal{O}_E^*)) .$$

On the other hand we get a map

$$(4.8) \quad k^S: \text{Hom}_{\Omega_{\mathbb{Q}}} (R_{\Gamma}^S / T(R_{\Gamma}), \pm 1) \rightarrow E^S(\Gamma)$$

which takes  $f$  into the class of  $\prod g^{(\ell)}$ , where  $g^{(\ell)}$  is the compositum

$$R_{\Gamma}^S \cap \text{Ker } d_{\ell} \rightarrow R_{\Gamma}^S / T(R_{\Gamma}) \xrightarrow{f} \pm 1 \rightarrow W_{\ell} .$$

Then we have

Theorem 5    Suppose that  $N/K$  is tame.    Then

$$h^S((0)_{\mathbb{Z}(\Gamma)}) = k^S(W(N/K)) .$$

Remark    One can define a group

$$E(\Gamma) = \prod_{\ell} \text{Hom}_{\Omega_{\mathbb{Q}}} (\text{Ker } d_{\ell}, W_{\ell}) / (\prod_{\ell} R_{\ell}^S) (\text{Hom}_{\Omega_{\mathbb{Q}}}^+ (R_{\Gamma}, \mathcal{O}_E^*)) ,$$

which maps surjectively onto  $\prod_{\ell} E_{\ell}(\Gamma)$  - sometimes with

non-trivial kernel, as Cassou-Nogues has shown, and

which also maps surjectively onto  $E^S(\Gamma)$ . The analogue of

the last two theorems for this "better" group remains

unproven, except for some special cases, partly due to Cassou-Nogues.

Examples Let  $\Gamma = H_{4\ell}^r$  be the generalised quaternion group of order  $4\ell^r$ ,  $\ell$  an odd prime. The groups  $E_\ell(\Gamma)$  and  $E^S(\Gamma)$  may be identified. They both are vector spaces over the field of 2 elements of dimension  $r$ , and this is also the structure of  $\text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma^S / T(R_\Gamma), \pm 1)$ . If  $\ell \equiv -1 \pmod{4}$  then  $k_\ell = k^S$  is a bijection, if  $\ell \equiv +1 \pmod{4}$  it is null. Thus for  $\ell \equiv +1 \pmod{4}$  our theorems tell us that the module invariant  $h_\ell((0)_{\mathbb{Z}(\Gamma)})$  in the non-trivial group  $E_\ell(\Gamma)$  does vanish. For  $\ell \equiv -1 \pmod{4}$ , and in conjunction with Theorem 18 of §14, we obtain a different type of non-trivial information. (For the case  $K = \mathbb{Q}$  see already [F3]).

## §5. Examples

We first mention one more general theorem, which is really classical. Let  $\Gamma^{\text{ab}}$  be the commutator quotient of  $\Gamma$ . The surjection  $\Gamma \rightarrow \Gamma^{\text{ab}}$  yields a surjection  $D(\mathbb{Z}(\Gamma)) \rightarrow D(\mathbb{Z}(\Gamma^{\text{ab}}))$ . If  $\Gamma$  is Abelian, and  $N/\mathbb{Q}$  is tame then one knows that  $0 \cong \mathbb{Z}(\Gamma)$ , i.e., we have a normal integral basis (over  $\mathbb{Z}$ ). (Indeed the Galois Gauss sums



are resolvents). Hence we have

Theorem 6    Let  $K = \mathbb{Q}$ , with  $N/\mathbb{Q}$  tame.    Then

$$(0)_{\mathbb{Z}(\Gamma)} \in \text{Ker}[D(\mathbb{Z}(\Gamma)) \rightarrow D(\mathbb{Z}(\Gamma^{\text{ab}}))] \quad .$$

Turning to explicit results for tame extensions with particular groups, these are of two types, as already illustrated at the end of the preceding section for  $\Gamma = H_{4\ell}^r$ . Firstly we may get a quite rigid connection between module invariants and symplectic root numbers. Theorems 4 and 5 give a general background to this, leading e.g. to the root number interpretation for  $H_{4\ell}^r$ ,  $\ell \equiv -1 \pmod{4}$ . The very first theorem of this kind, for  $\Gamma = H_8$ , the quaternion group of order 8, and  $K = \mathbb{Q}$  (cf. [F2]), which in a way started off this whole line of research, actually turns out not to be a special case of our theorems 4 and 5. It can however now be derived effortlessly directly from our Theorems 1 and 2. For a statement of the result, and for another proof involving a suggestive and interesting local approach see Martinet's talk (cf. [M4]).

The case  $\ell \equiv 1 \pmod{4}$  at the end of the last section indicates that Galois module structure does not always suffice for an interpretation of symplectic root numbers. This is a principal motivation for considering additional structure in terms of Hermitian forms over group rings. This however lies outside the scope of these lectures.

The second type of theorem is a normal integral basis theorem, asserting that under certain hypotheses

$(0)_{\mathbb{Z}(\Gamma)} = 1$ . Our general theorems 3, 4, 5 and 6 are of course approximate normal integral basis theorems, in that they restrict  $(0)_{\mathbb{Z}(\Gamma)}$  to a "small" subgroup of  $\text{Cl}(\mathbb{Z}(\Gamma))$ .

To get the actual equation  $(0)_{\mathbb{Z}(\Gamma)} = 1$  one uses one of three basic methods, or variants of these. (i) Apply Theorem 3, showing that  $D(\mathbb{Z}(\Gamma)) = 1$  for particular  $\Gamma$  - e.g.  $\Gamma$  dihedral of order  $2^n$  (cf. [FKW]) or of order  $2\ell$ ,  $\ell$  an odd prime. (The normal integral basis theorem in the latter case, for  $K = \mathbb{Q}$ , was actually proved by Martinet (cf. [ML]) before this whole theory existed). (ii) Use the map

$$G_\Gamma: D(\mathbb{Z}(\Gamma)) \rightarrow D(\mathbb{Z}(\Gamma^{\text{ab}})) \times \prod_{\ell} E_{\ell}(\Gamma).$$

If  $G_\Gamma$  can be shown to be injective, and if there are no irreducible symplectic characters, then in the case  $K = \mathbb{Q}$  we get  $(0)_{\mathbb{Z}(\Gamma)} = 1$ . This works for some metabelian groups

(cf. [F6], and some unpublished results of P. Cassou-Nogues and of M. Taylor). (iii) Apply Theorems 1 and 2 directly and derive some new procedures for certain classes of groups - work of M. Taylor on p-groups goes in this direction.

We end this section with the

Conjecture  $(0)_{\mathbb{Z}(\Gamma)}^2 = 1$  when  $K = \mathbb{Q}$ .

## §6. Conductors

Corresponding to the involution on  $\mathcal{O}(\Gamma)$  we have an involution - on its classgroup. If  $M$  is a locally free  $\mathcal{O}(\Gamma)$ -module, then  $(\bar{M}) = (M^*)^{-1}$ , the inverse in  $\text{Cl}(\mathcal{O}(\Gamma))$  of the dual, or "contragredient"  $M^*$  of  $M$ . With respect to the given representation of  $\Gamma$  as Galois group we have

Theorem 7. Suppose that all prime divisors of order  $(\Gamma)$  are non-ramified in  $N/K$  and denote by  $\mathfrak{f}(\chi)$  the conductor of  $\chi \in R_\Gamma$ . Then  $\{\mathfrak{f}(\chi)\}$  is a family of invariants for  $(0) (\bar{0}) \in \text{Cl}(\mathcal{O}(\Gamma))$ .

Corollary (and source of counter-examples)

If  $(0)_{\mathcal{O}(\Gamma)} = 1$  then, for each  $\chi \in R_\Gamma$ ,  $\mathfrak{f}(\chi)$  becomes a

principal ideal of  $^0_{K(\chi)}$ .

Recall that  $K(\chi)$  is the field of values of  $\chi$  over  $K$ .

Note At the appropriate places in Parts II and III we shall see how the theorems of Part I follow from those on resolvents and Galois Gauss sums.

## Part II. Resolvent theory

### §7. The basic connections

The results of this section will imply Theorem 1. We first indicate how the Galois group acts on resolvents and this will give us the first part of that theorem. The deeper second part will then be seen to follow from two other theorems on resolvents to be stated here. The first of these, relating them to module structure, is quite elementary, but the second one, establishing the connections with Galois Gauss sums, lies very deep, and is at the core of the whole theory.

Recall the definition of  $(a|\chi)$  (cf. (3.1)), and of  $\text{Det}_\chi$  (in §2). Restrict  $\text{Det}_\chi$  to  $\Gamma$  and compose it with  $\pi$ . We get a continuous Abelian character of  $\Omega_K$ , which by abuse

of notation we shall here again denote by  $\text{Det}_\chi$ . Then

$$(7.1) \quad (a|\chi^{\omega^{-1}})^\omega = (a|\chi) \text{Det}_\chi(\omega), \quad \text{for } \omega \in \Omega_K,$$

and more generally, if  $k \subset K$

$$(7.2) \quad N_{K/k}(a|\chi^{\omega^{-1}})^\omega = N_{K/k}(a|\chi)(v_{k/K} \text{Det}_\chi)(\omega), \quad \text{for } \omega \in \Omega_k,$$

where  $v_{k/K}: \text{Hom}(\Omega_K, \mathbb{C}^*) \rightarrow \text{Hom}(\Omega_k, \mathbb{C}^*)$  is the transfer. These equations, in conjunction with [M3] 2, Theorem 7.2, now imply the first part of Theorem 1.

We also note for later reference that

$$(7.3) \quad (a^\lambda|\chi) = (a|\chi) \text{Det}_\chi(\lambda) \quad \text{for } \lambda \in K(\Gamma)^*.$$

One can now proceed either idele theoretically, or ideal - and module theoretically, corresponding to the two descriptions (2.1) and (2.2) of  $\text{Cl}(\mathcal{O}(\Gamma))$ . Although we shall lay the emphasis on the first approach, we shall indicate briefly also the second one - each offers its own advantages.

We shall have to extend the notion of resolvent even further. It is clear in principle that it can be defined in the context of commutative rings. Here we are specifically concerned with local (or semilocal) completions. Let then  $p$  be a prime divisor of a subfield  $k$  of  $K$ . If  $a \in K_p(\Gamma)$   
 $= N_p (= N \otimes_k k_p)$ , i.e.  $a$  is a free generator of  $N_p$

over  $K_p(\Gamma)$ , then we can define the resolvent  $(a|\chi)$ , and similarly for  $k \subset F \subset K$  also  $N_{K/F}(a|\chi)$ , in essentially the same way as in §3. For  $E$  big enough, these will be in  $E_p^*$  ( $E_p = E \otimes_k k_p$ ). We shall specifically be interested in the case when  $a \sigma_p(\Gamma) = 0_p$ , i.e., when  $a$  generates a local normal integral basis at  $p$ .

More generally we shall look at products of completions, with  $p$  running over some set  $S$ . For  $S$  finite, no further comment is required. We consider the only other case which we shall need, namely  $S$  the set of all prime divisors (say in  $\mathbb{Q}$ ). We are now considering adele rings  $\text{Ad}(K)$ ,  $\text{Ad}(N)$  etc. For an adele  $\alpha$  of  $N$ , i.e., for  $\alpha \in \text{Ad}(N)$ , we again define

$$(\alpha|\chi) = \det \sum \alpha^\gamma T(\gamma)^{-1}, \quad N_{K/k}(\alpha|\chi) = \prod_{\sigma} (\alpha|\chi^{\sigma^{-1}})^{\sigma},$$

just as in (3.1), (3.2), provided of course that  $\alpha$  generates a normal basis of  $\text{Ad}(N)/\text{Ad}(K)$ , i.e., that

$$(7.4) \quad \begin{cases} \alpha_p K_p(\Gamma) = N_p, & \text{for all } p, \\ \alpha_p \sigma_p(\Gamma) = 0_p, & \text{for almost all } p. \end{cases}$$

Then  $(\alpha|\chi) \in J(E)$ . Formulae (7.1) - (7.3) extend in the obvious manner. Moreover via the embedding  $N \subset \text{Ad}(N)$ , the original resolvents may be viewed as adele resolvents.



Finally for local components we have

$$(7.5) \quad (\alpha|\chi)_p = (\alpha_p|\chi).$$

The ideal theoretical counterpart to adèle resolvents are the resolvent-modules  $(\mathcal{O}:\chi)$ . Note that, for given  $\chi$ , the resolvents  $(a|\chi)$ ,  $a \in N$  span a one-dimensional  $K(\chi)$ -subspace of  $\bar{\mathbb{Q}}$  (or of  $E$ ). This follows from (7.1). We define  $(\mathcal{O}:\chi)$  to be the  $\mathcal{O}_{K(\chi)}$ -module generated by the  $(a|\chi)$  with  $a \in \mathcal{O}$ . This is then rank one, finitely generated. Analogously we let  $N_{K/k}(\mathcal{O}:\chi)$  be the  $\mathcal{O}_{k(\chi)}$ -module generated by the  $N_{K/k}(a|\chi)$  with  $a \in \mathcal{O}$  (use (7.2) and draw the same conclusions!). If now  $N/K$  is tame, then there exists an adèle  $\alpha$  of  $N$ , so that for all  $p$ ,  $\alpha_p \mathcal{O}_p(\Gamma) = \mathcal{O}_p$ , and the connection with resolvent modules is given by

$$(7.6) \quad \begin{cases} (\alpha|\chi)_p \mathcal{O}_{K(\chi),p} = (\mathcal{O}:\chi)_p \\ (N_{K/k}(\alpha|\chi)_p) \mathcal{O}_{k(\chi),p} = N_{K/k}(\mathcal{O}:\chi)_p \end{cases}.$$

The next theorem describes the class of  $\mathcal{O}$  in terms of resolvents.

Theorem 8.    Suppose  $N/K$  to be tame.

(i) Let  $a \in N$ ,  $a K(\Gamma) = N$ . Let  $\alpha \in \text{Ad}(N)$ ,  
 $\alpha_p \mathcal{O}_p(\Gamma) = \mathcal{O}_p$ , for all  $p$ . Write



$$f(\chi) = (\alpha|\chi) (a|\chi)^{-1}$$

whence

$$N_{K/\mathbb{Q}} f(\chi) = N_{K/\mathbb{Q}} (\alpha|\chi) \cdot N_{K/\mathbb{Q}} (a|\chi)^{-1}.$$

Then  $f \in \text{Hom}_{\Omega_K} (R_\Gamma, J(E))$  and the class of  $f$  in  $\text{Cl}(\mathcal{O}(\Gamma))$  is  $(0)_{\mathcal{O}(\Gamma)}$ , and the class of  $N_{K/\mathbb{Q}} f$  in  $\text{Cl}(\mathbb{Z}(\Gamma))$  is  $(0)_{\mathbb{Z}(\Gamma)}$

(ii) With  $a$  as above, assume moreover that for all prime divisors  $p$  of order  $(\Gamma)$  we have  $a_p(\Gamma) = 0_p$ . Write  $b(\chi) = (\alpha:\chi) (a|\chi)^{-1}$ . Then  $\{b(\chi)\}$  is a family of invariants for  $(0)_{\mathcal{O}(\Gamma)}$ , and  $\{N_{K/\mathbb{Q}} b(\chi)\}$  one for  $(0)_{\mathbb{Z}(\Gamma)}$

We indicate the proof of (i), the idele theoretic version of the theorem. Go back to the description of  $(M) \in \text{Cl}(\mathcal{O}(\Gamma))$  given after (2.2). We now have  $M = 0$ ,  $V = N$ ,  $v = a$ . Then the adele  $\alpha$  of the theorem is of form  $\alpha = a\beta$ ,  $\beta$  an idele of  $K(\Gamma)$ . Thus  $(0)_{\mathcal{O}(\Gamma)}$  is represented by  $f$ , with  $f(\chi) = \text{Det}_\chi(\beta)$ . But by (7.3), or rather its extension to adeles we see that  $\text{Det}_\chi(\beta) = (\alpha|\chi) (a|\chi)^{-1}$ . This yields the stated description of  $(0)_{\mathcal{O}(\Gamma)}$ . For  $(0)_{\mathbb{Z}(\Gamma)}$  apply (2.8).

Now we come to the connection with Galois Gauss sums. This, as we shall see, looks neater in terms of resolvent

modules - possibly because we do not yet have the full story.

Theorem 9. Suppose that  $N/K$  is tame.

(i) Let  $\alpha \in \text{Ad}(N)$ ,  $\alpha \circ_p(\Gamma) = 0_p$  for all  $p$ . Let  
 $u(\chi) = \tau(\chi) N_{K/\mathbb{Q}}(\alpha|\chi)^{-1}$ . Then

$$u \in \text{Hom}_{\Omega_{\mathbb{Q}}} (R_{\Gamma}, U(E)).$$

(ii)  $\tau(\chi) \circ_{\mathbb{Q}(\chi)} = N_{K/\mathbb{Q}}(\circ:\chi)$ .

It is now clear that Theorem 1. is a consequence of the last two theorems. We shall only give an outline of the strategy of proof for Theorem 9, using most of the theory presented in the next few sections (see §10).

Remark Theorem 9, say in its adelic form, can be extended to the wild case. One can only demand that  $\alpha_p \circ_p(\Gamma) = 0_p$  at the tame primes, and one can then only assert that  $u \in \text{Hom}_{\Omega_{\mathbb{Q}}} (R_{\Gamma}, U'(E))$ , where  $U'(E)$  consists of those ideles which are units at the tame prime divisors.

## §8. Change of field or of group

This section contains a down to earth, explicit

account of the topic in the title. We shall avoid at this stage bringing in new concepts, in accordance with our aim to give a quick and accessible introduction to the essential results, rather than a formally presented theory. The appropriate formal background for the proper theoretical setting of these results will be briefly outlined in the appendix (which the reader can omit!).

In the sequel let  $A_L$  be one of the three following functors of number fields  $L$ .

$$(8.1) \quad \begin{cases} (i) & A_L = L. \\ (ii) & A_L = \prod_P o_{L,P} \text{ (product over all prime} \\ & \text{divisors } P \text{ of } L) \\ (iii) & A_L = o_{L,p}, \text{ where } p \text{ is a prime divisor} \end{cases}$$

of a number field  $k$ , and in this case  $L$  is restricted to extension fields of  $k$ .

Let  $N, K, \Gamma$  be as before, with  $k \subset K$ . In case (ii) assume  $N/K$  to be tame, in case (iii) to be tame above  $p$ .

We consider the maps

$$(8.2) \quad \chi \mapsto (a|\chi) \quad (\chi \in R_\Gamma)$$

where

$$a \in A_K(\Gamma) = A_N$$

(i.e.,  $a$  generates a "normal basis of  $A_N$ "). It is

important for the interpretation of the theorems in this section, that the maps (8.2), for varying  $a$ , coincide exactly with the maps

$$(8.3) \quad \chi \mapsto (a_o | \chi) \text{Det}_{\chi}(\lambda)$$

with  $a_o$  fixed,  $a_o A_K(\Gamma) = A_N$  and with  $\lambda$  varying over  $A_K(\Gamma)^*$  (i.e.,  $K(\Gamma)^*$  in case (i),  $U(o(\Gamma))$  in case (ii),  $o_p(\Gamma)^*$  in case (iii)).

Let  $\Delta$  be a normal subgroup of  $\Gamma$ ,  $F = N^{\Delta}$  its fixed field, and write  $\Sigma = \Gamma/\Delta$ . Thus  $\Sigma \cong \text{Gal}(F/K)$ . Let  $\ell: R_{\Sigma} \rightarrow R_{\Gamma}$  be the lifting of characters.

Theorem 10. Assume in case (8.1) (ii) that  $N/K$  is tame,  
in the case (8.1) (iii) tame above  $p$ . If  $a A_K(\Gamma) = A_N$  then  
 $t_{L/F}(a) A_K(\Sigma) = A_F$ , where  $t_{L/F}$  is the trace. Also, for  
 $\chi \in R_{\Sigma}$

$$(a | \ell\chi)_{N/K} = (t_{L/F}(a) | \chi)_{F/K}.$$

Remark on notation. We indicate resolvents with respect to  $N/K$  by subscripts as above - strictly speaking they depend on  $\pi$ .

Proof. Obvious.

Next let  $F$  be any number field containing  $K$ , let

$$\pi(\Omega_F) = \Delta \subset \Gamma. \quad \text{Then } \Delta \cong \text{Gal}(NF/F).$$

Theorem 11. In case (8.1) (ii) assume that  $N/K$  is tame and that furthermore each prime divisor  $P$  of  $K$  is non-ramified either in  $N$  or in  $F$ . In case (8.1) (iii) make the corresponding assumption just above  $p$ . Then given  $a \in A_N$ ,

$b \in A_{NF}$  so that

$$a A_K(\Gamma) = A_N, \quad b A_F(\Delta) = A_{NF},$$

$\exists \lambda \in A_F(\Gamma)^*$  with

$$(a|\chi)_{N/K} \text{Det}_\chi(\lambda) = (b|(\chi|\Delta))_{NF/F},$$

for all  $\chi \in R_\Gamma$ .

Here  $(\chi|\Delta)$  is the restriction of  $\chi$  to  $\Delta$ .

Outline of proof. We consider the induced  $\Gamma$ -module

$\text{Map}_\Delta(\Gamma, A_{NF})$  of the  $\Delta$ -module  $A_{NF}$ . This is an  $A_F$ -algebra by pointwise operation on maps e.g.  $f_1 f_2(\gamma) = f_1(\gamma) f_2(\gamma)$ .

Moreover  $\Gamma$  acts by algebra automorphisms.

On the other hand consider the  $A_F$ -algebra  $A_N \otimes_{A_K} A_F$ , with  $\Gamma$  acting via the tensor factor  $A_N$ . Then we have a homomorphism

$$(8.4) \quad \theta: A_N \otimes_{A_K} A_F \rightarrow \text{Map}_\Delta(\Gamma, A_{NF})$$

of algebras and  $\Gamma$ -modules, where  $\theta(x \otimes y)(\gamma) = x^\gamma y$ . In view of the hypotheses made, this is an isomorphism.

With  $b$  as given in the theorem let  $f_b \in \text{Map}_\Delta(\Gamma, A_{NF})$  be defined by

$$f_b(\gamma) = \begin{cases} b^\gamma, & \gamma \in \Delta \\ 0, & \gamma \notin \Delta, \gamma \in \Gamma \end{cases}.$$

Identifying the two modules in (8.4), via  $\theta$ , we see that

$$f_b A_F(\Gamma) = A_N \otimes_{A_K} A_F,$$

while on the other hand, with  $a$  as given, we also have

$$(a \otimes 1) A_F(\Gamma) = A_N \otimes_{A_K} A_F.$$

Hence

$$(8.5) \quad f_b = (a \otimes 1)^\lambda, \quad \lambda \in A_F(\Gamma)^*.$$

To form "resolvents" assume our big field  $E$  to contain  $F$  and  $N$ . In  $(A_N \otimes_{A_K} A_E)^*$  we then have the equation

$$(8.6) \quad \text{Det}_\chi \left( \sum_{\gamma \in \Gamma} f_b^\gamma \gamma^{-1} \right) = \text{Det}_\chi \left( \sum_{\gamma \in \Gamma} (a \otimes 1)^\gamma \gamma^{-1} \right) \cdot \text{Det}_\chi(1 \otimes \lambda).$$

Now let  $g: N \otimes_K E \rightarrow E$  be the map  $g(x \otimes y) = xy$ . Denote also by  $g$  the induced maps  $A_N \otimes_{A_K} A_E \rightarrow A_E$ . Then, recalling

the definition of  $f_b$ , it follows that

$$g(\text{Det}_\chi \left( \sum_{\gamma \in \Gamma} f_b^\gamma \gamma^{-1} \right)) = (b | (\chi | \Delta))_{NF/F}$$

while trivially

$$g(\text{Det}_\chi \left( \sum_{\gamma \in \Gamma} (a \otimes 1)^\gamma \gamma^{-1} \right)) = (a | \chi)_{N/K},$$

$$g(\text{Det}_\chi (1 \otimes \lambda)) = \text{Det}_\chi (\lambda).$$

The theorem is now seen to follow from (8.6) on applying  $g$ .

We note a Corollary, to be used subsequently.

Corollary    In case (iii) (so that each prime divisor  $P$  of  $K$ , above  $p$ , is non-ramified either in  $N$  or in  $F$ ), we have

$$v_q((a | \chi)_{N/K}) = v_q((b | (\chi | \Delta))_{NF/F}),$$

for all  $\chi \in R_\Gamma$ , and all prime divisors  $q$  of  $E$ , above  $p$ .

( $a, b$  as in the theorem). In particular if  $(\chi | \Delta) = 0$  then

$$v_q((a | \chi)_{N/K}) = 0.$$

Here  $v_q: E_q^* \rightarrow \mathbb{Z}$  is the standard valuation.

Next let  $\Delta$  be again a subgroup of  $\Gamma$ , and let now  $F = N^\Delta$ .

Then again  $\Delta \cong \text{Gal}(N/F)$ . For  $\phi \in R_\Delta$  denote by  $\phi_*$  the induced character of  $\Gamma$ .

Theorem 12.    Assume in case (8.1) (ii) that  $N/K$  is tame, in



case (8.1) (iii) that  $N/K$  is tame above  $p$ . Let

$$a \ A_K(\Gamma) = A_N, \quad b \ A_F(\Delta) = A_N$$

and let  $\{c_i\}$  be a free basis of  $A_F/A_K$  and  $\{\sigma\}$  a right transversal of  $\Omega_F$  in  $\Omega_K$  (or of  $\Delta$  in  $\Gamma$ ). Then for some  $\lambda \in A_K(\Delta)^*$

$$(a|\phi_*)_{N/K} \text{Det}_\phi(\lambda) = N_{F/K} (b|\phi) \cdot (\det c_i^\sigma)^{\deg(\phi)}.$$

Outline of proof Let  $\{a_i\}$  be a free basis of  $A_N$  over  $A_K(\Delta)$  and  $\{\sigma\}$  a right transversal of  $\Omega_F$  in  $\Omega_K$ . If, say,  $T: \Delta \rightarrow GL_n(E)$  is a representation, we consider the block matrix with row index  $\sigma$ , column index  $i$  whose  $\sigma, i$  entry is the matrix  $T(\sum_{\delta \in \Delta} a_i^{\delta\sigma} \delta^{-1})$ . Its determinant will only depend on the character  $\phi$  of  $\Delta$ , corresponding to  $T$ , on the choice of  $\{a_i\}$ , and on the choice of  $\{\sigma\}$ . We shall denote it by  $\text{Det}_\phi(\{a_i\})$ . Note in passing that this is a generalisation both of resolvents, and of discriminants. Note also that for the definitions we only need tameness hypotheses on  $N/F$ , not on  $N/K$ .

Remark: We have been a bit vague as to where the matrix  $T(\sum_{\delta \in \Delta} a_i^{\delta\sigma} \delta^{-1})$  lies. In fact we may view it as a matrix over  $A_E$ .

The dependence of  $\text{Det}_\phi(\{a_i\})$  on the choice of  $\{\sigma\}$  can be neglected. A different choice of transversal is reflected by a factor  $\text{Det}_\phi(\delta)$ , with  $\delta$  fixed in  $\Delta$ . On the other hand if  $\{a'_i\}$  is another free basis of  $A_N$  over  $A_K(\Delta)$  then

$$(8.7) \quad \text{Det}_\phi(\{a'_i\}) = \text{Det}_\phi(\{a_i\}) \text{Det}_\phi(\lambda), \quad \lambda \in A_K(\Delta)^*.$$

Now we choose particular bases  $\{a_i\}$ . First suppose that  $A_K(\Gamma) = A_N$ . Then, with  $\{\sigma\}$  as above,  $\{a_i^{\sigma^{-1}}\}_\sigma$  is a free basis of  $A_N$  over  $A_K(\Delta)$ . Here of course the  $\sigma \in \Omega_K$  can be replaced by their images  $\pi(\sigma) \in \Gamma$ . An analysis of induced representations then shows that

$$(8.8) \quad \text{Det}_\phi(\{a_i^{\sigma^{-1}}\}) = (a|\phi_*)_{N/K}.$$

Next with  $b, \{c_i\}$  as in the theorem we take  $a_i = bc_i$ .

Then

$$(8.9) \quad \text{Det}_\phi(\{bc_i\}) = N_{F/K} (b|\phi)_{N/F} \cdot (\det c_i^\sigma)^{\deg(\chi)}.$$

The theorem now follows from (8.7) - (8.9).

## §9. Kummer extensions

Here  $K$  is assumed to contain the primitive  $n$ -th roots of unity and we assume that  $\Gamma \cong \text{Gal}(N/K)$  is cyclic of order  $n$ . A radical  $x$  of  $K$  in  $N$  (or of  $K_p$  in  $N_p$ , where now

$p$  is a prime divisor of  $K$ ) is an element of  $N^*$  with  $x^n \in K^*$  (an element of  $N_p^*$  with  $x^n \in K_p^*$ ). The valuation  $v_p: K_p^* \rightarrow \mathbb{Z}$  can be extended uniquely to a homomorphism, from the group of radicals of  $K_p^*$  in  $N_p^*$ , into  $\mathbb{Q}$ . If  $\chi$  is a character of  $\Gamma$  of degree 1, which we may view as a homomorphism of  $\Gamma$  into the group of  $n$ -th roots of unity, then the elements  $x \in N$ , with  $x^\gamma = x\chi(\gamma)$  for all  $\gamma \in \Gamma$  form a one dimensional  $K$ -subspace  $V_\chi$ . All non zero elements of  $V_\chi$  (of  $V_{\chi,p}$ ) are radicals and their values under  $v_p$  form a unique coset of  $\mathbb{Q} \bmod \mathbb{Z}$ . Write  $r(\chi, p)$  for the least non negative rational in this coset. Thus  $0 \leq r(\chi, p) < 1$ .

Now assume that  $p$  is finite and that  $n$  is a unit at  $p$ . Via class field theory we get from  $\chi$  a character of  $K_p^*$  whose restriction to the group  $U_p$  of  $p$ -adic units we denote by  $\chi_{(p)}$ . Then there is a unique rational  $s(\chi, p)$ ,  $0 \leq s(\chi, p) < 1$  so that for all  $u \in U_p$

$$\chi_{(p)}(u) \equiv u^{-(Np-1)s(\chi, p)} \pmod{p}.$$

Now let a  $\sigma_p(\Gamma) = \sigma_p$ . Then  $(a|\chi)$  is a radical, and  $v_p((a|\chi))$  will be independent of the particular choice of  $a$  within the stated conditions. We have

Theorem 13 (i)  $v_p((a|\chi)) = r(\chi, p)$  (Kummer criterion)

$$(ii) \ v_p((a|\chi)) = s(\chi, p) \quad (\text{class field criterion}).$$

The proof of (i) is not hard. One then derives (ii) from (i), using all the properties of the local norm residue symbol.

#### §10. Outline proof of Theorem 9

We take the theorem in form (i). With  $\alpha$  as in the theorem, we write

$$u(\chi) = \tau(\chi) N_{K/\mathbb{Q}}(\alpha|\chi)^{-1}.$$

Then

$$(10.1) \quad u \in \text{Hom}(R_\Gamma, J(E)).$$

We divide the assertion of the theorem into two parts, proving separately that

$$(10.2) \quad u \in \text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma, J(E))$$

and that

$$(10.3) \quad u \in \text{Hom} (R_\Gamma, U(E)),$$

where  $U(E)$  is the group of unit ideles.

Now (10.2) follows immediately from the way in which  $\Omega_{\mathbb{Q}}$  acts on  $N_{K/\mathbb{Q}}(\alpha|\chi)$ , (see (7.2), or rather its generalisation), and on  $\tau(\chi)$  (cf. [M3] 2, Theorem 7.2). Compare

here with the proof of Theorem 1.

We are then left with the proof of (10.3). This proceeds by a number of reduction steps.

1<sup>st</sup> step Immediately from (10.1) one notes that it will suffice to prove that

$$(10.4) \quad u(\chi) \in U(E)$$

for a set of generators  $\chi$  of  $R_\Gamma$ . We shall take for this the induced characters of abelian characters of subgroups.

2<sup>nd</sup> step We reduce the proof to that of (10.4), for any number field  $K$  as base field, and for  $\chi$  abelian. This is done by using the induction properties of  $\tau(\chi)$  on the one hand (cf. [M3] 2, Theorem 8.1), and of  $(\alpha|\chi)$  on the other (see Theorem 12, or rather a slight strengthening of it).

3<sup>rd</sup> step One reduces to semilocal components. More precisely, take  $\chi$  abelian and let  $p$  be a rational prime. In the evaluation of  $v_q(\tau(\chi))$  where  $q$  is a prime divisor of  $E$  above  $p$  one can replace  $\tau(\chi)$  by the local Gauss-sums of the prime divisor  $P$  of  $K$ , above  $p$ . Thus one has to compare this with the values  $v_q((\alpha|\chi))$ .

4<sup>th</sup> step The evaluation of the  $v_q(\tau(\chi))$ , which

essentially goes back to Stickelberger (compare [C] 3.6, 3.7, 3.8).

5<sup>th</sup>-step If  $\chi$  abelian,  $\text{order}(\chi) = p^s m$ ,  $(m, p) = 1$ ,  $p$  as in the 3<sup>rd</sup>. step, then  $\chi = \phi\psi$ ,  $\text{order}(\phi) = p^s$ ,  $\text{order}(\psi) = m$ . By hypothesis of tame ramification,  $\phi$  is non-ramified at all prime divisors of  $K$  above  $p$ , and so the virtual character  $\chi - \psi$  vanishes on all corresponding inertia groups. By the Corollary to Theorem 11, we may replace  $\chi$  by  $\psi$ , i.e. we may assume  $(\text{order}(\chi), p) = 1$ .

6<sup>th</sup>-step If  $\chi$  abelian,  $(\text{order}(\chi), p) = 1$  then  $K(\chi)/K$  is non-ramified above  $p$ . By Theorem 11 we may, for the evaluation of  $v_q((\alpha|\chi))$ , assume that  $K = K(\chi)$ .

7<sup>th</sup>-step Evaluate  $v_q((\alpha|\chi))$  by Theorem 13 (ii). The Theorem now follows by comparison with what came out of the 4<sup>th</sup> step.

#### §11. Relation to Artin Conductor

In this section let  $p$  be a finite prime divisor of  $K$ . As  $\text{Det}_{\chi+\bar{\chi}} = 1$ , it follows that  $(a|\chi+\bar{\chi})_{N/K} \in K(\chi + \bar{\chi})$ , for  $a \in N$ , with an analogous result for  $a \in N_p$ . Denote by  $f(\chi)$  the Artin conductor.

Theorem 14. Suppose that  $N/K$  is tame at  $p$  and let

$a \in \mathcal{O}_p(\Gamma) = \mathcal{O}_p$ . Then

$$(a | \chi + \bar{\chi})_{\mathcal{O}_{K(\chi + \bar{\chi})}, p} = \delta(\chi)_p \mathcal{O}_{K(\chi + \bar{\chi}), p} \quad .$$

The proof uses methods similar to that of Theorem 9, but is much easier and less deep. Thus e.g. only Theorem 13 (i) will be needed.

Theorem 14 together with a computation for resolvents yielding a formula of type

$$(a | \chi + \bar{\chi}) = \text{Det}_{\chi}(\lambda_a)$$

then yields Theorem 7.

#### §11a. Congruence and Signature properties

We first return to the subject matter of §4. Indeed our next theorem is one of the ingredients in the proof of Theorems 4 and 5. The symbol  $L_E$  denotes again the product of prime ideals of  $\mathcal{O}_E$  above  $\ell$ .

Theorem 15 Suppose that  $N/K$  is tame above the rational prime  $\ell$  (i.e., tamely ramified at all prime divisors of  $K$  above  $\ell$ ). Then, if  $a \in \mathcal{O}_{\ell}(\Gamma) = \mathcal{O}_{\ell}$ , we have

$$(a | \chi) \equiv 1 \pmod{L_E}$$



for all  $\chi \in \text{Ker } d_\ell$ .

If actually  $N/K$  is non-ramified above  $\ell$  then  $\sum a^\gamma \gamma^{-1}$  is a unit of  $\mathcal{O}_\ell(\Gamma)$  and hence  $\text{Det}_\chi(\sum a^\gamma \gamma^{-1}) \equiv 1 \pmod{L_E}$ . If there is ramification one uses Theorem 12 to reduce to the case  $\chi = \phi - \psi$ ,  $\deg(\phi) = \deg(\psi) = 1$ ,  $(\text{order } \phi, \ell) = 1$ . In this case the result is then again easily verified.

Next we turn to signature properties. If  $p$  is a real prime divisor of  $K$ , then  $W_p(\chi)$  denote the corresponding local root number (cf. [T]).

Theorem 16    Let  $p$  be a real prime divisor of  $K$ , and let  
 $a \in K_p(\Gamma) = N_p$ .    Then for all  $\chi \in R_\Gamma^S$   

$$\text{sign}_p(a|\chi) = W_p(\chi)$$

for any prime divisor  $P$  of  $K(\chi)$  above  $p$ .

(Thus  $\text{sign}_p(a|\chi)$  is independent of the choice of  $P$ , as the choice of  $a$ ).

From the theorem one deduces the

Corollary    For each  $\chi \in R_\Gamma^S$ ,  $N_{K/\mathbb{Q}}(a|\chi)$  is either totally  
positive or totally negative, and

$$\text{sign } N_{K/\mathbb{Q}}(a|\chi) = W_{\infty}(\chi).$$

Theorem 2 is now clearly a consequence of this Corollary and of [M3] 2, Theorem 7.4.

For the proof of Theorem 16 one first shows that indeed  $\text{sign}_P(a|\chi)$ , for  $\chi \in R_{\Gamma}^S$ , is independent of the choice of  $a$  or of  $P$ . One then verifies the equation with a particular convenient choice of  $a$  in the  $K_p$ -algebra  $N_p$ .

### Part III. Galois Gauss sums and Root numbers

#### §12. Congruence properties of Galois Gauss sums

We once more return to the subject matter of §4. Let  $V^{(\ell)}$  denote the group of roots of unity in  $\bar{\mathbb{Q}}$  of order prime to  $\ell$ .

Theorem 17 Suppose that  $N/K$  is tame. Then there is a unique  $y_{\ell} \in \text{Hom}_{\Omega_{\mathbb{Q}}}(\text{Ker } d_{\ell}, V^{(\ell)})$  so that

$$y_{\ell}(\chi) \equiv \tau(\chi) \pmod{L_E},$$

for all  $\chi \in \text{Ker } d_{\ell}$ . If moreover  $\chi \in R_{\Gamma}^S \cap \text{Ker } d_{\ell}$  then  
 $y_{\ell}(\chi) = 1$ , i.e.,  $\tau(\chi) \equiv 1 \pmod{L_E}$ .

Outline of Proof It suffices to show, for some set of generators  $\chi$  of  $\text{Ker } d_\ell$  (of  $R_\Gamma^S \cap \text{Ker } d_\ell$ ) that  $\tau(\chi)$  is congruent mod  $L_E$  to a root of unity in  $V^{(\ell)}$  (to 1). Using induction the proof reduces to the case of Abelian or quaternion characters. One then localises and has to do a bit of work.

Theorems 4 and 5 can now be deduced from Theorems 1, 2 and 15, 17. We illustrate the main points in terms of Theorem 5. First, theorem 1 describes  $(0)_{\mathbb{Z}(\Gamma)}$  by the invariants  $b(\chi) = (\tau(\chi) N_{K/\mathbb{Q}}(a|\chi)^{-1})$ . Restricting  $\chi$  to  $R_\Gamma^S$ , we can replace this by  $b(\chi) = (\tau(\chi) N_{K/\mathbb{Q}}(a|\chi)^{-1} W(\chi))$ . By Theorem 2, the generator of this principal ideal is totally positive. One deduces that  $h^S((0))$  is represented by  $g \in \text{Hom}_{\Omega_{\mathbb{Q}}} (R_\Gamma^S \cap \text{Ker } d_\ell, W_\ell)$ , where  $g(\chi)$  is the class mod  $L_E$  of  $N_{K/\mathbb{Q}}(a|\chi) \cdot \tau(\chi)^{-1} W(\chi)$ , for all  $\chi \in R_\Gamma^S \cap \text{Ker } d_\ell$ . By Theorems 15 and 17 this is the same as the class of  $W(\chi)$  mod  $L_E$ . Thus  $g(\chi)$  also represents  $k^S(W(N/K))$ .

### §13. Properties of Galois Gauss sums and root numbers

We have used the  $\tau(\chi)$  to derive results on Galois module structure. One can however change one's point of view and in turn apply our general theorems to obtain

information on the  $\tau(\chi)$ .

Note that in the proofs, specifically that of the basic Theorem 9, the (known) fact that the  $\tau(\chi)$  are algebraic integers (first proved by Dwork) was not used. For "tame"  $\chi$  this result follows evidently from Theorem 9 without any further computations. For, by the Theorem,  $\tau(\chi)$  generates a module which by its definition consists of algebraic integers only.

Theorem 9 determines the map  $\chi \mapsto \tau(\chi)$  (for tame  $\chi$ ) to within an  $\Omega_{\mathbb{Q}}$ -homomorphism  $\chi \mapsto y(\chi)$  into global units. If one observes that  $\tau(\chi)\overline{\tau(\chi)}$  is rational this becomes a homomorphism into roots of unity. The problem then arises, what further intrinsic properties will determine  $\chi \mapsto \tau(\chi)$  uniquely.

One can ask corresponding questions also for the local Galois Gauss sums ([M3], 2, §4), and the local root numbers ([T]) - at least for symplectic  $\chi$ . The local approach moreover gives some hope also in the wild case - at least modulo roots of unity. It is already clear however, even for the interpretation of global symplectic root numbers that additional elements of structure are needed, beyond that of the integers as a Galois module - specifically

"Hermitian Galois module structure" defined via the trace form. This topic however lies outside the scope of these notes.

Another result which we can prove, again based on Theorem 9, is that the "non Abelian Jacobi sum"

$$\tau(\chi)^{\deg(\psi)} \tau(\psi)^{\deg(\chi)} / \tau(\chi\psi)$$

(for tame  $\chi$  and  $\psi$ ) is an algebraic integer.

#### §14. The range of symplectic root numbers

The problem considered in this section is that referred to in §4. We now vary the map  $\pi$  of (1.1), i.e., the representation of  $\Gamma$  as a Galois group of a tame extension. Corresponding to each  $\pi$  we get an element - given by the root numbers - of  $\text{Hom}_{\Omega_{\mathbb{Q}}} (R_{\Gamma}^S / T(R_{\Gamma}), \pm 1)$ , and the problem is to decide which elements are of this form. We shall discuss this in a particular case only, taking  $K = \mathbb{Q}$ , and  $\Gamma = H_{4m}$  the quaternion group of order  $4m$ , with  $m$  odd. For these groups every automorphism of  $\Gamma$  keeps the  $\Omega_{\mathbb{Q}}$ -orbits in  $R_{\Gamma}^S$  fixed, hence also keeps  $\text{Hom}_{\Omega_{\mathbb{Q}}} (R_{\Gamma}^S / T(R_{\Gamma}), \pm 1)$  fixed. Thus the element of that group corresponding to a particular  $\pi$ , will only depend on  $N = \overline{\mathbb{Q}}^{\text{Ker } \pi}$ , and we denote it by  $W(N)$ . Thus  $W(N)$  is the map:  $\chi \mapsto W(N, \chi)$  in the classical notation.

Let  $F'$  be a tame, absolutely cyclic field of degree 4. To avoid complications assume that the quadratic subfield  $F$  of  $F'$  has class number and discriminant prime to  $m$ . Then, for  $\Gamma = H_{4m}$ , we have

Theorem 18. For every  $W \in \text{Hom}_{\Omega_Q}(R_\Gamma^S/T(R_\Gamma), \pm 1)$ , there exist infinitely many fields  $N$ , tame and normal with  $\text{Gal}(N/Q) \cong \Gamma$ , so that  $N \supset F'$  and  $W(N) = W$ .

Outline of proof 1) The  $\Omega_Q$ -conjugacy classes of irreducible symplectic characters  $\psi$  of  $H_{4m}$  correspond biuniquely to the divisors  $d > 1$  of  $m$ , under a map  $\psi \mapsto d_\psi$  where  $\psi$  is the character of a representation lifted from a faithful representation of the quotient group  $H_{4d}$  ( $d = d_\psi$ ) of  $H_{4m}$ . We shall then write  $W(N, \psi) = W_d(N)$  when  $d = d_\psi$ . We thus have to show:

$$(14.1) \quad \left\{ \begin{array}{l} \text{given a map } f \text{ from the set of divisors } d > 1 \text{ of} \\ m \text{ to } \pm 1, \text{ there exist infinitely many } N, \text{ tame} \\ \text{and normal with } \text{Gal}(N/Q) \cong \Gamma, \text{ and } N \supset F', \text{ so} \\ \text{that } W_d(N) = f(d) \text{ for all } d. \end{array} \right.$$

2) Let  $\mu$  be the quadratic idele class character of

$F$  corresponding to its extension  $F'$ . Let  $\phi$  be an idele class character of  $F$  of order  $m$ , not ramified at the prime divisors of  $m$ , with  $\phi(J(\mathbb{Q})) = 1$ . View  $\phi\mu$  as character of  $\Omega_F$ , and let  $\psi_d$  be the character of  $\Omega_{\mathbb{Q}}$  induced by  $(\phi\mu)^{m/d}$ . Then, writing  $N$  for the fixed field of  $\phi\mu$  we see that  $N$  is tame and normal over  $\mathbb{Q}$  with  $\text{Gal}(N/\mathbb{Q}) \cong H_{4m}$ , and contains  $F'$ . Moreover  $\psi_d = \psi$  is an irreducible symplectic character with  $d = d_\psi$ .

Let  $s_d(\phi)$  be the number of rational prime factors  $p$  of  $d(\phi^{m/d})$  which are inert in  $F$ . Then by a computation given in [F5] (Theorem 2),

$$W_d(N) = (-1)^{s_d(\phi)}.$$

We thus have to show

$$(14.2) \quad \left\{ \begin{array}{l} \text{Given } f \text{ as in (14.1) there exist infinitely} \\ \text{many idele class characters } \phi \text{ of } F \text{ of order } m, \\ \text{not ramified at the prime divisors of } m, \text{ with} \\ \phi(J(\mathbb{Q})) = 1 \text{ and with } f(d) = (-1)^{s_d(\phi)} \text{ for all } d. \end{array} \right.$$

3) For  $S$  a finite set, write

$$\sigma(S) = (-1)^{\text{Card}(S)}.$$

Given  $f$  as in (14.1) one can show the existence of a



family  $\{S_d\}$  of sets of natural numbers, one set  $S_d$  corresponding to each divisor  $d > 1$  of  $m$ , so that (i)  $d|d'$  implies  $S_d \subset S_{d'}$ , (ii)  $d = d'd''$ ,  $(d', d'') = 1$  implies  $S_d = S_{d'} \cup S_{d''}$ . (iii)  $\sigma(S_d) = f(d)$ . In the sequel the symbol  $S_1$  will be the empty set. Fix such a family  $\{S_d\}$  once and for all.

4) Let  $P$  be an injective map of  $S_m$  into the set of natural primes not dividing  $m$ , so that (i)  $P_{(j)}$  is inert in  $F$  and non-ramified in  $F'$ , (ii)  $P_{(j)} \equiv -1 \pmod{m}$ . There are clearly infinitely many such maps. The proof of (14.2) now reduces to

(14.3)  $\left\{ \begin{array}{l} \text{Given } \{S_d\}, \text{ and } P, \text{ as above, there exists} \\ \text{an idele class character } \phi \text{ of } F \text{ of order } m \\ \text{with } \phi(J(\mathbb{Q})) = 1 \text{ so that (i) a prime } P_{(j)} \text{ will} \\ \text{divide } \phi(\phi^{m/d}) \text{ if and only if } j \in S_d, \text{ (ii)} \\ p|\phi(\phi), p \notin S_m \text{ implies that } p \nmid m \text{ and that} \\ p \text{ splits in } F. \end{array} \right.$

In fact for such a  $\phi$  we will have  $s_d(\phi) = \text{card}(S_d)$ .

5) Given  $\{S_d\}$ , and  $P$ , observe first that for each  $j \in S_m$  there is a unique greatest divisor  $g(j) = g \geq 1$  of  $m$  with  $j \notin S_g$ . For each  $j \in S_m$ , we can then choose a

residue class character  $\delta_j \bmod P_{(j)} \mathcal{O}_F$  of order  $m/g(j)$ . View  $\delta_j$  as a character of the local units at  $P_{(j)}$ , and extend it to a character, again denoted by  $\delta_j$ , of the group of unit ideles  $U(F)$  of  $F$ , so that  $\delta_{j,p} = 1$  for prime divisors  $p$  other than  $P_{(j)}$ . Next choose a natural prime  $q \equiv 1 \pmod{m}$ , which splits in  $F$ , and a residue class character  $\delta$  of  $\mathcal{O}_F/q\mathcal{O}_F$  of order  $m$ , which takes values 1 on rational residue classes. View  $\delta$  as a character of  $U(F)$ , ramified only at the prime divisors above  $q$ . We can moreover fix  $q$  and  $\delta$  so that

$$\prod_j \delta_j(\eta) \delta(\eta) = 1$$

for a fundamental unit  $\eta$  of  $F$ .

Let  $h$  be the class number of  $F$ . If  $\alpha$  is an idele of  $F$  then  $\alpha^h \equiv u \pmod{F^*}$ ,  $u \in U(F)$ . Put  $\phi(\alpha) = \delta(u) \prod_j \delta_j(u)$ . This defines a unique idele class character  $\phi$  with all the required properties.

### §15. Symplectic root numbers for wild extensions

The interpretation of symplectic root numbers depends on the fact that in the tame case  $W(\chi^\omega) = W(\chi)$  for all  $\omega \in \Omega_Q$ . In the wild case this need no longer be so. We shall give here a recipe for infinitely many normal disjoint

wild extensions of  $\mathbb{Q}$  in which the symplectic root numbers are not invariant under transition to  $\Omega_{\mathbb{Q}}$ -conjugate characters, generalising an example given in [F4]. The Galois groups are quaternion groups  $H_{4\ell}$  of order  $4\ell$ , with  $\ell$  an odd prime which is totally ramified. This implies of course  $\ell \equiv 1 \pmod{4}$ .

The method is based on a Lemma, which is the global analogue to a local result in [M3] (2. Proposition 6.1).

Lemma Let  $\chi$  be a real valued character with trivial determinant. Then, for  $\omega \in \Omega_{\mathbb{Q}}$ ,

$$\frac{W(\chi^\omega)}{W(\chi)} = \frac{(N\delta(\chi)^{1/2})^\omega}{N\delta(\chi)^{1/2}}.$$

Thus  $W(\chi^\omega) = W(\chi)$  for all  $\omega$  precisely when  $N\delta(\chi)$  is a square.

Indeed as  $W(\chi) = \pm 1$ , we have  $W(\chi)^\omega = W(\chi)$ . Also always  $N\delta(\chi^\omega) = N\delta(\chi)$ . Thus, expressing  $W$  in terms of  $\tau$ ,  $W_\infty$  and  $N\delta^{1/2}$ , we have

$$\frac{W(\chi^\omega)}{W(\chi)} = \frac{W(\chi^\omega)}{W(\chi)^\omega} = \frac{\tau(\chi^\omega)}{\tau(\chi)^\omega} \frac{W_\infty(\chi^\omega)}{W_\infty(\chi)^\omega} \frac{(N\delta(\chi)^{1/2})^\omega}{N\delta(\chi)^{1/2}}.$$

But, as  $\text{Det}_\chi = 1$ , we have  $\tau(\chi^\omega) = \tau(\chi)^\omega$ ,  $W_\infty(\chi^\omega) = W_\infty(\chi)$ , hence the result.

Denote by  $\psi$  an irreducible symplectic character of  $H_{4\ell}$ .

Theorem 19    Let  $\ell \equiv 1 \pmod{4}$  be a prime number and  $F'$  a cyclic field of degree 4 over  $\mathbb{Q}$  in which  $\ell$  is totally ramified, and so that the class number of the quadratic subfield of  $F'$  is prime to  $\ell$ . Then there exist infinitely many normal fields  $N$  containing  $F'$ , in which  $\ell$  is totally ramified and so that

$$f(N/\mathbb{Q}, \psi) = \ell^3 \ell', \quad (\ell', \ell) = 1$$

i.e.,

$$W(N/\mathbb{Q}, \psi^\omega) \neq W(N/\mathbb{Q}, \psi), \quad \text{for some } \omega.$$

Proof    We follow the general technique developed in [F4].

Let  $F$  be the quadratic subfield of  $F'$ , and  $\rho$  a residue character of  $\mathcal{O}_F / \ell \mathcal{O}_F$  of exact order  $\ell$ . We then have to find infinitely many idele class characters  $\phi$  of  $F$ , such that

$$(15.1) \quad \phi \text{ is of exact order } \ell$$

$$(15.2) \quad \phi \text{ restricted to the local units of } F \text{ at } \ell \text{ is } \rho$$

$$(15.3) \quad \phi(J(\mathbb{Q})) = 1.$$

One shows that if  $F_\phi$  is the corresponding class field, then  $N = F'F_\phi$  has the required properties.

View  $\rho$  as a character of  $U(F)$ , ramified only above  $\ell$ . Choose a prime  $p \equiv 1 \pmod{\ell}$ , splitting in  $F$  and so that there is a residue class character  $\mu$  of  $\mathcal{O}_F/p\mathcal{O}_F$  which is 1 on rational residue classes and for which  $\mu\rho(\eta) = 1$ ,  $\eta$  a fundamental unit of  $F$ . There are infinitely many such  $p$ . Given  $\mu$  and  $\rho$  we can then construct a  $\phi$  which only ramifies at  $\ell$  and at  $p$ , whose restriction to  $U(F)$  is  $\mu\rho$  and so that  $\phi(J(\mathbb{Q})) = 1$ ,  $\phi^\ell = 1$ . (Here  $\mu$  is always of order  $\ell$ ).

### Appendix

#### §16. Once more: Change of field or of group

Just as in §2, the representation of  $\Gamma$  as a Galois group is not assumed here and is irrelevant. We are simply concerned with pairs, consisting of a finite group and a number field, and study the formal behaviour of various associated objects.

First of all we have to consider more general sets of homomorphisms than the group  $\text{Hom}_{\Omega_F}$ . Let then  $F$  be a number field,  $\Gamma$  a finite group,  $X$  some  $\Omega_{\mathbb{Q}}$ -module written multiplicatively. We consider pairings

$$\phi : R_\Gamma \times \Omega_F \rightarrow X$$

so that

$$(16.1) \quad \phi(\chi + \chi', \omega) = \phi(\chi, \omega) \phi(\chi', \omega),$$

$$(16.2) \quad \phi(\chi, \omega\omega') = \phi(\chi, \omega) \phi(\chi, \omega'),$$

$$(16.3) \quad \phi(\chi^{\sigma^{-1}}, \omega)^{\sigma} = \phi(\chi, \omega),$$

for  $\omega, \omega' \in \Omega_F$ ,  $\sigma \in \Omega_{\mathbb{Q}}$ ,  $\chi, \chi' \in R_{\Gamma}$ . We denote by

$\text{Hom}_{\Omega_F, \phi}(R_{\Gamma}, X)$  the set of homomorphisms  $f: R_{\Gamma} \rightarrow X$  of groups with

$$(16.4) \quad f(\chi^{\omega^{-1}})^{\omega} = f(\chi) \phi(\chi, \omega),$$

for all  $\omega \in \Omega_F$ ,  $\chi \in R_{\Gamma}$ . If  $\phi_1, \phi_2$  are two such pairings then multiplication in  $\text{Hom}(R_{\Gamma}, X)$  yields a pairing

$\text{Hom}_{\Omega_F, \phi_1} \times \text{Hom}_{\Omega_F, \phi_2} \rightarrow \text{Hom}_{\Omega_F, \phi_1 \phi_2}$ . In particular,  $\text{Hom}_{\Omega_F, \phi}$  is either empty or else is a coset of  $\text{Hom}_{\Omega_F}$  in  $\text{Hom}$ .

(i) Restriction of base fields.

Let  $k$  be a subfield of the number field  $K$ . We have already considered the norm map  $N_{K/k}$  (cf (2.6)) on the groups  $\text{Hom}_{\Omega_K}(R_{\Gamma}, X)$ . One can show that the map  $N_{K/k}$ , for  $X = J(E)$ , maps  $\text{Det}(U(\mathcal{O}(\Gamma)))$  into  $\text{Det}(U(\mathcal{O}_k(\Gamma)))$  (similarly for  $\text{Det}(K(\Gamma)^*)$  etc). Hence we get, via (2.1), a homomorphism

$$N_{K/k}: \text{Cl}(\mathcal{O}(\Gamma)) \rightarrow \text{Cl}(\mathcal{O}_k(\Gamma)).$$

Comparing with restriction of scalars, one gets, for a

locally free  $\mathcal{O}(\Gamma)$ -module  $M$  of rank  $r$ , the formula

$$(16.5) \quad (M)_{\mathcal{O}_k(\Gamma)} = (\mathcal{O}(\Gamma))_{\mathcal{O}_k(\Gamma)}^r \cdot N_{K/k}((M)_{\mathcal{O}(\Gamma)}).$$

When  $k = \mathbb{Q}$  the first factor on the right vanishes and we get (2.8).

We define also a map

$$N_{K/k}: \text{Hom}_{\Omega_K, \phi}(R_\Gamma, X) \rightarrow \text{Hom}_{\Omega_K, v\phi}(R_\Gamma, X)$$

by choosing a right transversal  $\{\sigma\}$  of  $\Omega_K$  in  $\Omega_k$  and setting

$$(16.6) \quad (N_{K/k} f)(\chi) = \prod_{\sigma} f(\chi^{\sigma^{-1}})^{\sigma}.$$

Here  $v\phi(\chi, ) = v_{k/K} \phi(\chi, )$  is the image of  $\phi(\chi, ) \in \text{Hom}(\Omega_K, X)$

under the transfer map. A different choice of  $\{\sigma\}$  leads to

a different map  $N'_{K/k}$ , but only to within a factor

$\chi \mapsto \phi(\chi, \omega_o)$  where  $\omega_o$  is fixed in  $\Omega_K$ .

(ii) Extension of base fields.

Let  $F$  be a number field containing  $K$ . We have a natural embedding  $i_{K/F}: \text{Hom}_{\Omega_K} \hookrightarrow \text{Hom}_{\Omega_F}$  (and analogous when a pairing  $\phi$  is present), which acts in the obvious way on  $\text{Det}(U(\mathcal{O}(\Gamma)))$ , hence induces a map  $i_{K/F}: \text{Cl}(\mathcal{O}(\Gamma)) \rightarrow \text{Cl}(\mathcal{O}_F(\Gamma))$ . One then has

$$(16.7) \quad i_{K/F}((M)_{\mathcal{O}(\Gamma)}) = (M \otimes \mathcal{O}_F)_{\mathcal{O}_F(\Gamma)}.$$

(iii) Transition to quotient groups.



Let  $\Sigma = \Gamma/\Delta$ ,  $\Delta$  a normal subgroup of  $\Gamma$ . Lifting

$\ell: R_\Sigma \rightarrow R_\Gamma$  of characters yields homomorphisms

$$\lambda_\Sigma^\Gamma : \text{Hom}_{\Omega_K}(R_\Gamma, X) \rightarrow \text{Hom}_{\Omega_K}(R_\Sigma, X)$$

which takes e.g.  $\text{Det}(U(\mathcal{O}(\Gamma)))$  into  $\text{Det}(U(\mathcal{O}(\Sigma)))$ . It thus induces a homomorphism  $\lambda_\Sigma^\Gamma$  on class groups, and we have

$$(16.8) \quad \lambda_\Sigma^\Gamma((M)_{\mathcal{O}(\Gamma)}) = (M^\Delta)_{\mathcal{O}(\Sigma)} .$$

Analogous when a  $\phi$  is present.

(iv) Restriction to subgroups.

Here  $\Delta$  is a subgroup of  $\Gamma$ . Induction of characters

$\chi \mapsto \chi_*$  is a homomorphism  $R_\Delta \rightarrow R_\Gamma$  which yields maps

$$\rho_{\Gamma/\Delta} : \text{Hom}_{\Omega_K}(R_\Gamma, X) \rightarrow \text{Hom}_{\Omega_K}(R_\Delta, X),$$

and analogously when a  $\phi$  is present. Again one can show

that e.g. for  $X = J(E)$ , the map  $\rho_{\Gamma/\Delta}$  takes  $\text{Det}(U(\mathcal{O}(\Gamma)))$  into  $\text{Det}(U(\mathcal{O}(\Delta)))$ , hence yields a homomorphism

$\rho_{\Gamma/\Delta} : \text{Cl}(\mathcal{O}(\Gamma)) \rightarrow \text{Cl}(\mathcal{O}(\Delta))$ . Now we have

$$(16.9) \quad \rho_{\Gamma/\Delta}((M)_{\mathcal{O}(\Gamma)}) = (M)_{\mathcal{O}(\Delta)} .$$

(v) Induction.

With  $\Delta$  and  $\Gamma$  as under (iv), restriction  $R_\Gamma \rightarrow R_\Delta$  of characters yields maps

$$i_{\Delta/\Gamma}: \text{Hom}_{\Omega_K}(R_{\Delta}, X) \rightarrow \text{Hom}_{\Omega_K}(R_{\Gamma}, X)$$

(and analogously when a pairing  $\phi$  is present). We get an induced homomorphism  $i_{\Delta/\Gamma}: \text{Cl}(\mathcal{O}(\Delta)) \rightarrow \text{Cl}(\mathcal{O}(\Gamma))$ , and have

$$(16.10) \quad i_{\Delta/\Gamma}((M)_{\mathcal{O}(\Delta)}) = (M_*)_{\mathcal{O}(\Gamma)},$$

where  $M_*$  is the  $\Gamma$ -module induced by  $M$ .

### §17. Functorial behaviour of resolvent classes and module classes

Now we assume again as given a surjection  $\pi: \Omega_K \rightarrow \Gamma$ , with  $N = \overline{\mathcal{Q}}^{\text{Ker } \pi}$ . If first  $\Sigma = \Gamma/\Delta$  (as in 16. (iii)) then by composition we get a surjection  $\pi_{\Sigma}: \Omega_K \rightarrow \Sigma$ , and  $\overline{\mathcal{Q}}^{\text{Ker } \pi_{\Sigma}} = N^{\Delta} = F$ , say. If  $N/K$  is tame we have from (16.8)

$$(17.1) \quad \lambda_{\Sigma}^{\Gamma}((0)_{\mathcal{O}(\Gamma)}) = (\mathcal{O}_F)_{\mathcal{O}(\Sigma)}.$$

Next let  $\Delta$  be any subgroup of  $\Gamma$ , let again  $F = N^{\Delta}$ . If  $N/K$  is tame, then by (16.5), (16.9)

$$(17.2) \quad (\mathcal{O}_F(\Delta))_{\mathcal{O}(\Delta)} \cdot N_{F/K}((0)_{\mathcal{O}_F(\Delta)}) = \rho_{\Gamma/\Delta}((0)_{\mathcal{O}(\Gamma)}).$$

Next let  $F$  be some number field containing  $K$  and let  $\pi(\Omega_F) = \Delta$ . Suppose that  $N/K$  is tame and that each prime divisor of  $K$  is non-ramified either in  $N$  or in  $F$ . Then

$$(17.3) \quad i_{\Delta/\Gamma}((o_{NF})_{o_F(\Delta)}) = i_{K/F}((0)_{o(\Gamma)}) .$$

This will follow from (16.7), (16.10) and the isomorphism (cf. (8.4))

$$\theta : o_N \otimes_o o_F \xrightarrow{\cong} \text{Map}_{\Delta}(\Gamma, o_{NF}) .$$

We now return to §8, using the notation established there. The surjection  $\pi: \Omega_K \rightarrow \Gamma$  gives rise to a particular pairing  $\phi = \text{Det}$ , where  $\phi(\chi, \omega) = \text{Det}_{\chi}(\pi\omega)$ . The map  $\chi \mapsto (a|\chi)$ , where  $a_{A_K(\Gamma)} = a_N$  then lies in  $\text{Hom}_{\Omega_K, \text{Det}}(R_{\Gamma}, X)$  for some suitable  $X$ . More precisely  $X = E^*$ ,  $J(E)$ ,  $E_p^*$  for  $A_L = L$ ,  $\prod_p o_{L,p}, o_{L,p}$  respectively. Moreover these maps coming from resolvents, for varying  $a$  with  $a_{A_K(\Gamma)} = a_N$ , form one orbit under the action of  $\text{Det}(A_K(\Gamma)^*)$ , to be denoted by  $r(A_N/A_K)$  (abuse of notation).

Thus

$$r(A_N/A_K) \in \text{Hom}_{\Omega_K, \text{Det}}(R_{\Gamma}, X) / \text{Det}(A_K(\Gamma)^*) .$$

The theorems of §8 can now be reformulated in terms of the maps defined in the preceding section 16, and the resolvent classes  $r(A_N/A_K)$ .

Example: Theorem 10 asserts that  $\lambda_{\Sigma}^{\Gamma} r(A_N/A_K) = r(A_F/A_K)$ .

Theorem 11 that  $i_{K/F} r(A_N/A_K) = i_{\Delta/\Gamma} r(A_{NF}/A_F)$ . A similar interpretation, involving  $N_{F/K}$  and  $\rho_{\Gamma/\Delta}$ , can be given to

Theorem 12. This would however require some further definitions which we shall not give here.

## REFERENCES

- [C] Coates, p-adic L-functions and Iwasawa's theory, Durham Symposium.
- [F1] A. Fröhlich, Resolvents, Discriminants and Trace invariants, Journ. Alg. 4 (1966), 643-662.
- [F2] A. Fröhlich, Artin root numbers and normal integral bases for quaternion fields, Invent. Math. 17, 143-166 (1972).
- [F3] A. Fröhlich, Module invariants and root numbers for quaternion fields of degree  $4\ell^r$ , Proc. Camb. Phil. Soc. 76 (1974), 393-399.
- [F4] A. Fröhlich, Artin root numbers, conductors and representations for generalised quaternion groups, Proc. London. Math. Soc. 28 (1974), 402-438.
- [F5] A. Fröhlich, Artin rootnumbers for quaternion characters, Symp. Math. 15 (1975), 393-363.
- [F6] A. Fröhlich, A normal integral basis theorem, Journ. Alg 39(1976), 131-137.
- [F7] A. Fröhlich, Resolvents and Trace form, Math. Proc. Camb. Phil. Soc. 78 (1975), 185-210.
- [F8] A. Fröhlich, Galois module structure and Artin L-functions, Soc. Math. France, Asterisque 24-25, (1975), 9-13.
- [F9] A. Fröhlich, Galois module structure and Artin L-functions, Proc. Internat. Congress of Mathematicians, Vancouver 1974, 351-356.

- [F10] A. Fröhlich, Arithmetic and Galois module structure for tame extensions, to appear in Crelle.
- [FKW] A. Fröhlich, M. Keating and S. Wilson, The Class group of quaternion and dihedral 2-groups, Mathematika 21 (1974), 64-71.
- [M.1] J. Martinet, Sur l'arithmétique des extensions Galoisiennes à groupe de Galois diédral d'ordre  $2p$ , Ann. Inst. Fourier (Grenoble) 19 (1969) 1, 1-80.
- [M.2] J. Martinet, Bases normales et constante de l'équation fonctionnelle des fonctions  $L$  d'Artin, Sem. Bourbaki 1973/74, exposé 450.
- [M.3] J. Martinet, Character theory and Artin  $L$ -functions, Durham Symposium. '
- [M.4] J. Martinet,  $H_8$ , Durham Symposium.
- [S] J-P. Serre, Représentations Linéaires des Groupes Finis. 2<sup>me</sup> édition, Hermann, Paris, 1971.
- [T] J. Tate, Local constants, Durham Symposium.



# Modular forms of weight one and Galois representations

J.-P. Serre

(prepared in collaboration with C.J. Bushnell)

## PART I

### Introduction

- §1 Two-dimensional Galois Representations
- §2 Modular Forms
- §3 The Main Theorems
- §4 Proof of Theorem 2
- §5 Applications

## PART II

### Introduction

- §6 Cohomology and Liftings
- §7 Dihedral Representations
- §8 Representations with Prime Conductor
- §9 Modular Forms of Weight One on  $\Gamma_0(p)$



Part I of these notes is basically a résumé of [DS]. The principal result proved is that the Mellin transform of a (suitably normalised) newform of weight 1 (with character) is the Artin L-function of a two-dimensional linear representation of the Galois group of the rational numbers. The representations which arise in this way have a simple characterisation (modulo the Artin Conjecture), and one obtains a bijection between a set of newforms and a set of isomorphism classes of Galois representations.

Some applications of a general nature are given in §5. Part II deals with more explicit examples.

## §1. Two-dimensional Galois representations

Let  $\bar{\mathbb{Q}}/\mathbb{Q}$  denote an algebraic closure of the rational number field  $\mathbb{Q}$ , and let  $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ . Let  $\rho: G \rightarrow \text{GL}_2(\mathbb{C})$  denote a two-dimensional continuous complex linear representation of  $G$ . (Throughout, linear representations of  $G$  will be implicitly assumed continuous. Recall that, in this case, continuity means having open kernel, and hence finite image.) The map  $\sigma \mapsto \det(\rho(\sigma))$ ,  $\sigma \in G$ , is a one-dimensional linear representation of  $G$ , which we denote by:

$$\varepsilon = \det(\rho): G \rightarrow \mathbb{C}^\times.$$

Let  $c \in G$  be a "complex conjugation", or Frobenius at infinity; then  $c$  is of order 2 (and, by a theorem of Artin, is the only element of  $G$  of order 2, up to conjugation).

So, if  $\chi$  is a one-dimensional linear representation of  $G$ ,  $\chi(c) = \pm 1$ , and we say that  $\chi$  is odd if  $\chi(c) = -1$ .

Let  $N$  be the Artin conductor, and  $L(s, \rho)$  the Artin L-function, of the representation  $\rho$ . We refer to [Dur.M] for the definitions and basic properties of these. The conductor of  $\varepsilon = \det(\rho)$  divides  $N$  so that, via class field theory, we may regard  $\varepsilon$  as a Dirichlet character mod  $N$

$$\varepsilon: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times.$$

Then the representation  $\varepsilon$  of  $G$  is odd if and only if this Dirichlet character satisfies  $\varepsilon(-1) = -1$ .

For  $\rho$  such that  $\varepsilon$  is odd, define:

$$\Lambda(s, \rho) = N^{s/2} (2\pi)^{-s} \Gamma(s) L(s, \rho).$$

Then one knows that  $\Lambda$  extends to a meromorphic function on the whole  $s$ -plane, and has the functional equation:

$$\Lambda(1-s, \rho) = W(\rho) \cdot \Lambda(s, \bar{\rho}),$$

where  $\bar{\rho}$  is the contragredient of the representation  $\rho$ , and  $W(\rho)$  is a constant. The Artin Conjecture states that  $\Lambda(s, \rho)$  is a holomorphic function of  $s$ , for  $s \neq 0, 1$ . Recall that  $\Lambda(s, \rho)$  is holomorphic for  $s = 0, 1$  if  $\rho$  does not contain the

unit representation of  $G$ . We say that  $\rho$  satisfies condition (A) if:

(A): there exists a positive integer  $M$  such that, for all one-dimensional linear representations  $\chi$  of  $G$  with conductor prime to  $M$ ,  $\Lambda(s, \rho \otimes \chi)$  is a holomorphic function of  $s$  for  $s \neq 0, 1$ .

The representation  $\rho$  satisfies the condition (A) if, in particular, it is reducible or monomial (i.e. induced by a one-dimensional representation).

## §2. Modular Forms

In what follows, we use only holomorphic modular forms of one variable, and we describe them in classical terms; for interpretations (and generalisations) in the language of infinite-dimensional representations of  $GL(2)$ , see for instance [DA], [J-L], [WL].

2.1 Let  $H = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$  denote the complex upper half-plane, and  $GL_2^+(\mathbb{R})$  the group of  $2 \times 2$  real matrices with determinant  $> 0$ . Then  $GL_2^+(\mathbb{R})$  acts on  $H$  as a group of holomorphic automorphisms:

$$\sigma: z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta}, \quad \text{where } \sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2^+(\mathbb{R}).$$

Let  $f$  be a holomorphic function on  $H$ , and  $k$  a positive integer. For  $\sigma$  as above, define:

$$f|_k \sigma(z) = \det(\sigma)^{k/2} (\gamma z + \delta)^{-k} f\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right).$$

For fixed  $k$ ,  $\sigma : f \mapsto f|_k \sigma$  defines a group action of  $GL_2^+(\mathbb{R})$  on the space of holomorphic functions on  $H$ .

Let  $\Gamma = SL_2(\mathbb{Z})$ , and let  $\Gamma'$  be a subgroup of  $\Gamma$  of finite index. Let  $f$  be a holomorphic function on  $H$  such that  $f|_k \sigma = f$  for all  $\sigma \in \Gamma'$ . The group  $\Gamma'$  contains a matrix  $\begin{pmatrix} 1 & M \\ 0 & 1 \end{pmatrix}$ , for some positive integer  $M$ . Hence  $f(z + M) = f(z)$  for all  $z \in H$ , and so  $f$  has a "Fourier expansion at infinity":

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q_M^n, \quad q_M = e^{2\pi i z/M}.$$

We say that  $f$  is holomorphic (resp. vanishes) at infinity if  $a_n = 0$  for all  $n < 0$  (resp.  $n \leq 0$ ). If  $\sigma \in \Gamma$ , then  $f|_k \sigma|_k \sigma' = f|_k \sigma$ , for all  $\sigma' \in \sigma^{-1} \Gamma' \sigma$ . So, for any  $\sigma \in \Gamma$ ,  $f|_k \sigma$  also has a Fourier expansion at infinity. We say that  $f$  is holomorphic (resp. vanishes) at the cusps if  $f|_k \sigma$  is holomorphic (resp. vanishes) at infinity for all  $\sigma \in \Gamma$ .

Now let  $N$  be an integer  $\geq 1$ , and  $\epsilon$  a Dirichlet character mod  $N$ . Define:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N} \right\}.$$

A modular form on  $\Gamma_0(N)$  of type  $(k, \epsilon)$  is a holomorphic function  $f$  on  $H$  such that:

- (i)  $f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \epsilon(d)f$  for all  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$   
and  
(ii)  $f$  is holomorphic at the cusps.

Notice that (i) implies  $f|_k \Gamma' = f$  for some subgroup  $\Gamma'$  of  $\Gamma_0(N)$  of finite index, so that (ii) is meaningful. Also, the Fourier expansion of such a modular form is of the form:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \quad q = q_1 = e^{2\pi iz}.$$

The integer  $k$  in the type  $(k, \epsilon)$  is called the weight.

The weight and the character are related by:

$$\epsilon(-1) = (-1)^k,$$

since, if  $f$  is a modular form of type  $(k, \epsilon)$ ,

$$(-1)^{-k} f = f|_k \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \epsilon(-1)f.$$

Such a modular form is called a cusp form if it vanishes at the cusps. The modular forms on  $\Gamma_0(N)$  of type  $(k, \epsilon)$  form a complex vector space  $M(\Gamma_0(N), k, \epsilon)$ , and this has a subspace  $S(\Gamma_0(N), k, \epsilon)$ , consisting of the cusp forms. The subspace  $S$  has a canonical complement:

$$M(\Gamma_0(N), k, \epsilon) = E(\Gamma_0(N), k, \epsilon) \oplus S(\Gamma_0(N), k, \epsilon),$$

where  $E$  is the space spanned by the "Eisenstein series".

See [H, 24] or [Sch] for the definition of Eisenstein series in this context. The above decomposition of  $M$  is proved for  $k \geq 2$  in [Sch], and for  $k = 1$  in [P].

2.2 Hecke Operators: Let  $p$  denote a prime number, and  $f(z) = \sum_{n=0}^{\infty} a_n q^n$  a modular form on  $\Gamma_0(N)$  of type  $(k, \epsilon)$ . The Hecke operators  $T_p, U_p$  are defined by:

$$f|T_p = \sum_{n=0}^{\infty} a_{np} q^n + \epsilon(p) p^{k-1} \sum_{n=0}^{\infty} a_n q^{np} \text{ if } p \nmid N,$$

$$f|U_p = \sum_{n=0}^{\infty} a_{np} q^n \quad \text{if } p|N.$$

Then  $f|T_p, f|U_p$  are also modular forms on  $\Gamma_0(N)$  of type  $(k, \epsilon)$ , and they are cusp forms if  $f$  is a cusp form. See [Ogg] or [Sh].

2.3 Newforms: For a full discussion of newforms, see [Li] and the references therein. Suppose  $N'|N$ , and that  $\epsilon$  is a Dirichlet character mod  $N'$ . If  $f$  is a cusp form on  $\Gamma_0(N')$  of type  $(k, \epsilon)$ , and  $dN'|N$ , then  $z \mapsto f(dz)$  is a cusp form on  $\Gamma_0(N)$  of type  $(k, \epsilon)$ . The forms on  $\Gamma_0(N)$  which may be obtained in this way from divisors  $N'$  of  $N$ ,



$N' \neq N$ , span a subspace  $S^-(\Gamma_0(N), k, \epsilon)$  of  $S(\Gamma_0(N), k, \epsilon)$ .

This leads to a decomposition of  $S$ :

$$S(\Gamma_0(N), k, \epsilon) = S^-(\Gamma_0(N), k, \epsilon) \oplus S^+(\Gamma_0(N), k, \epsilon)$$

into subspaces orthogonal under the Petersson inner product, ([Ogg]). These subspaces are stable under the Hecke operators. The space  $S^+$  is spanned by the so-called newforms. A newform  $f = \sum a_n q^n$  is a non-zero cusp form, and it is an eigenvector of all the Hecke operators  $T_p, U_p$ :

$$f|T_p = \lambda_p f, \quad p \nmid N,$$

$$f|U_p = \lambda_p f, \quad p|N,$$

with  $\lambda_p \in \mathbb{C}$ . This implies that  $a_1 \neq 0$ , and that:

$$\lambda_p = a_1^{-1} a_p,$$

for all  $p$ . We shall say that a newform is normalised if  $a_1 = 1$ .

If two newforms have the same eigenvalues  $\lambda_p$ , for almost all  $p$ , they differ by a constant factor ([Li]).

(Using the connection with  $\ell$ -adic representations, one can even show that this holds when the forms have the same eigenvalues  $\lambda_p$  for a set of primes  $p$  of density  $> 7/8$ .)

Any cusp form on  $\Gamma_0(N)$  of type  $(k, \epsilon)$  can be written,



essentially uniquely, as a finite sum  $\sum_i f_i(d_i z)$ , where  $d_i N_i | N$ ,  $\varepsilon$  can be defined mod  $N_i$ , and  $f_i$  is a newform on  $\Gamma_0(N_i)$  of type  $(k, \varepsilon)$ .

To any modular form  $f = \sum_{n=0}^{\infty} a_n q^n$  of the above type, we can attach the Dirichlet series:

$$L_f(s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

The series  $L_f(s)$  converges in some right-hand half-plane.

One knows that it has an Euler product expansion if  $f$  is an eigenfunction of the Hecke operators. See [H,36] or [Ogg].

In particular, if  $f$  is a normalised newform of type  $(k, \varepsilon)$ , we have:

$$L_f(s) = \prod_{p \nmid N} (1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s})^{-1} \prod_{p|N} (1 - a_p p^{-s})^{-1}.$$

**2.4 Functional Equation:** For a modular form  $f$  on  $\Gamma_0(N)$ , the function:

$$\Lambda_f(s) = N^{s/2} (2\pi)^{-s} \Gamma(s) L_f(s)$$

extends to a meromorphic function on the whole  $s$ -plane, with the functional equation:

$$\Lambda_f(k-s) = i^k \Lambda_{f'}(s),$$

where  $k$  is the weight of  $f$ , and  $f' = f|_k W$  with  $W = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ , that is:

$$f'(z) = N^{-k/2} z^{-k} f(-1/Nz).$$

The only possible singularities of  $\Lambda_f$  are simple poles at  $s = 0$ ,  $k$ , and  $\Lambda_f$  is holomorphic if  $f$  vanishes at infinity. See [Sh] or [Ogg]. When  $f$  is a newform on  $\Gamma_0(N)$  of type  $(k, \epsilon)$ ,  $\Lambda_f(s)$  is holomorphic. The function  $f'$  is then a newform on  $\Gamma_0(N)$  of type  $(k, \bar{\epsilon})$ . One proves (cf. [Li, p.296]) that it is equal to  $c\bar{f}$ , where  $c$  is a constant, and  $\bar{f} = \sum \bar{a}_n q^n$ . In particular, the functional equation may be rewritten as:

$$\Lambda_f(k - s) = ci^k \Lambda_{\bar{f}}(s).$$

Notice the analogy between this and the functional equation of §1.

**2.5 Properties of Eigenvalues:** Let  $f = \sum a_n q^n$  be a cusp form on  $\Gamma_0(N)$  of type  $(k, \epsilon)$ , and let  $\sigma$  be an automorphism of the field  $\mathbb{C}$ . Define:

$$f^\sigma = \sum_{n=1}^{\infty} a_n^\sigma q^n.$$

In [DS, 2.7], using methods from algebraic geometry and the Tate curve, it is proved that:

- (i)  $f^\sigma$  is a cusp form on  $\Gamma_0(N)$  of type  $(k, \epsilon^\sigma)$ ;
- (ii) if the coefficients  $a_n$  are algebraic, they have bounded denominators;
- (iii) the eigenvalues of the Hecke operators  $T_p, U_p$ , on  $S(\Gamma_0(N), k, \epsilon)$  lie in the ring of integers of an algebraic number field (of finite degree over  $\mathbb{Q}$ ).

Alternatively, one may deduce these results from the classical theory as follows.

When  $k \geq 2$ , assertions (i) and (ii) follow from [Sh, 3.5.20, th. 3.52], which relies on the Eichler-Shimura isomorphism relating (cusp) forms of weight  $k$  with (parabolic) cohomology classes in the symmetric  $(k-2)$ -power of  $\mathbb{Z}^2$ . The case  $k = 1$  can be reduced to  $k \geq 2$  by the following trick. Let:

$$\Delta = q \cdot \prod_{n=1}^{\infty} (1 - q^n)^{24}, \text{ and}$$

$$Q = 1 + 240 \cdot \sum_{n=1}^{\infty} \sigma_3(n) q^n, \text{ where } \sigma_h(n) = \sum_{\substack{d>0 \\ d|n}} d^h.$$

Then  $Q, \Delta$ , are modular forms on  $\Gamma = \text{SL}_2(\mathbb{Z})$ , of weights

4, 12, respectively. The form  $\Delta$  vanishes at infinity, but not on  $H$ , while  $Q$  is non-zero at infinity. The map:

$$(Q, \Delta): f \longmapsto (Qf, \Delta f)$$

is an isomorphism between  $S(\Gamma_0(N), 1, \epsilon)$  and the space  $V_\epsilon$  consisting of pairs  $(g, h)$  where:

$$(a) \quad g \in S(\Gamma_0(N), 5, \epsilon), \quad h \in S(\Gamma_0(N), 13, \epsilon), \quad \text{and}$$

$$(b) \quad \Delta g = Qh.$$

The statement (ii) in weight 1 now follows from the case  $k \geq 2$ . Further, we see that  $\sigma$  induces a commutative diagram:

$$\begin{array}{ccc} V_\epsilon & \xrightarrow{\sim} & V_{\epsilon^\sigma} \\ (Q, \Delta) \downarrow \sim & & \downarrow \sim (Q, \Delta) \\ S(\Gamma_0(N), 1, \epsilon) & \longrightarrow & S(\Gamma_0(N), 1, \epsilon^\sigma) \end{array}$$

and hence a (semilinear) isomorphism  $S(\Gamma_0(N), 1, \epsilon) \stackrel{\sim}{=} S(\Gamma_0(N), 1, \epsilon^\sigma)$ . This proves (i) in weight 1.

To prove (iii), it is now enough to show that the eigenvalues of the  $T_p, U_p$ , on a given  $S(\Gamma_0(N), k, \epsilon)$  all lie in an algebraic number field. From the definition, it is clear that:

$$(f|T_p)^\sigma = f^\sigma|T_p, \quad (f|U_p)^\sigma = f^\sigma|U_p,$$

for  $f \in S(\Gamma_0(N), k, \epsilon)$ . Therefore, if  $\{\lambda_p\}$  is a system of

eigenvalues of the  $T_p, U_p$  on  $S(\Gamma_0(N), k, \epsilon)$ , so is  $\{\lambda_p^\sigma\}$ , for any automorphism  $\sigma$  of  $\mathbb{C}$  fixing the values of  $\epsilon$ . Since the space  $S(\Gamma_0(N), k, \epsilon)$  is finite-dimensional, there are only finitely many distinct systems  $\{\lambda_p^\sigma\}$  of eigenvalues, as  $\sigma$  ranges over the automorphisms of  $\mathbb{C}$  fixing the values of  $\epsilon$ . So (iii) holds for all  $k \geq 1$ .

### §3. The Main Theorems

3.1 We have said, in 2.4, that the Dirichlet series attached to a cusp form on  $\Gamma_0(N)$  is holomorphic and has a functional equation. The same applies to the other Dirichlet series obtained from this one by "twisting" with a Dirichlet character whose conductor is prime to  $N$ .

Conversely, suppose one starts with a Dirichlet series  $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ . If  $\chi$  is a Dirichlet character with conductor  $m_\chi$ , define

$$L_\chi(s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}, \quad \Lambda(s) = (2\pi)^{-s} \Gamma(s) L(s),$$

$$\Lambda_\chi(s) = (m_\chi^{-1} \cdot 2\pi)^{-s} \Gamma(s) L_\chi(s).$$

If  $\Lambda$ , and  $\Lambda_\chi$  for sufficiently many  $\chi$ , are holomorphic, bounded in vertical strips, with functional equations of the appropriate type, then  $f(z) = \sum_{n=1}^{\infty} a_n q^n$  is a cusp form

on some  $\Gamma_0(N)$ . This is a theorem of Weil, [W]; cf. [Li, th.8]. For more general results in this direction, see [WL] and [J-L].

A holomorphic Artin L-function  $\Lambda(s, \rho)$  is bounded in vertical strips ([WL, p.163]). Combining the functional equation of the  $\Lambda(s, \rho \otimes \chi)$  and the properties of the Artin root number ([Dur.T]) with [Li, th.8], one obtains:

Theorem 1 (Weil-Langlands) Let  $\rho$  be an irreducible two-dimensional complex linear representation of  $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  with conductor  $N$  and  $\varepsilon = \det(\rho)$  odd. Assume that  $\rho$  satisfies condition (A) of §1. Suppose  $L(s, \rho) = \sum_{n=1}^{\infty} a_n n^{-s}$ , and let  $f(z) = \sum_{n=1}^{\infty} a_n q^n$ . Then  $f$  is a normalised newform on  $\Gamma_0(N)$  of type  $(1, \varepsilon)$ .

In the other direction:

Theorem 2 (Deligne-Serre) Let  $f$  be a normalised newform on  $\Gamma_0(N)$  of type  $(1, \varepsilon)$ . Then there exists an irreducible two-dimensional complex linear representation  $\rho$  of  $G$  such that  $L_f(s) = L(s, \rho)$ . Further, the conductor of  $\rho$  is  $N$ , and  $\det(\rho) = \varepsilon$ .

Remark:

There are similar results, due to Hecke [H,36], for reducible two-dimensional representations  $\rho$  with  $\det(\rho) = \varepsilon$  and conductor  $N$ . These correspond to the normalised "primitive" Eisenstein series of type  $(1, \varepsilon)$  on  $\Gamma_0(N)$ .

3.2 The correspondences  $\rho \mapsto L(s, \rho)$ ,  $f \mapsto L_f(s)$  yield a bijection between the set of normalised newforms on  $\Gamma_0(N)$  of type  $(1, \varepsilon)$ , and the set of isomorphism classes of irreducible two-dimensional representations of  $G$  with conductor  $N$ , determinant character  $\varepsilon$ , satisfying condition (A). This gives a way of checking the Artin Conjecture in certain specific cases. Given a representation  $\rho$  of the appropriate kind, one can determine the coefficients  $a_n$  of its L-function, for  $n \leq B$ , say. One can then try to construct a modular form with Fourier coefficients  $a_n$ , for  $n \leq B$ . If  $B$  is sufficiently large, for example:

$$B \geq \frac{N}{12} \cdot \prod_{p|N} (1 + p^{-1}),$$

this form is uniquely determined, if it exists. The form then gives rise to a representation  $\rho_1$ , via Theorem 2. Then  $\rho$  satisfies the condition (A) if it is isomorphic to



$\rho_1$ . Otherwise, the Artin Conjecture is false.

3.3 A two-dimensional linear representation  $\rho$  of  $G$  gives rise to a projective linear representation,  $\tilde{\rho}$ , of  $G$ :

$$\begin{array}{ccc} G & \xrightarrow{\rho} & GL_2(\mathbb{C}) \\ & \searrow \tilde{\rho} & \downarrow \\ & & PGL_2(\mathbb{C}) \end{array}$$

where  $PGL_2(\mathbb{C}) = GL_2(\mathbb{C})/\mathbb{C}^\times$ . Notice that  $\det(\rho)$  is odd if and only if  $\tilde{\rho}(c) \neq 1$ , for a complex conjugation  $c \in G$ . The image of  $\tilde{\rho}$  is a finite subgroup of  $PGL_2(\mathbb{C})$ , and hence is one of the following:

- (i)  $C_n$  - cyclic of order  $n$ ;
- (ii)  $D_n$  - dihedral of order  $2n$ ,  $n \geq 2$ ;
- (iii) the alternating groups  $A_4, A_5$ , or the symmetric group  $S_4$ .

If  $\text{Im}(\tilde{\rho})$  is cyclic,  $\text{Im}(\rho)$  is abelian and hence  $\rho$  is reducible. Otherwise,  $\rho$  is irreducible. In the dihedral case, (A) is satisfied since  $\rho$  is induced from a one-dimensional representation of  $\text{Gal}(\bar{\mathbb{Q}}/K) \subset G$ , for some quadratic field  $K/\mathbb{Q}$ . The modular form attached to  $\rho$  is a linear combination of  $\theta$ -series of binary quadratic forms associated with  $K$  (cf.

[H,23])). We will discuss this case further in §7.

Tate has constructed a number of examples of representations  $\rho$  of type (iii); see Part II. For one of these, with conductor 133, and  $\text{Im}(\tilde{\rho}) \cong A_4$  he managed, with the aid of Atkin et al., to find a corresponding modular form, and so gave the first verification of the Artin Conjecture in a non-trivial case.

Recently, in [LB], Langlands has made a very important advance with case (iii) above. By representation theoretic arguments, involving descent properties of representations of  $\text{GL}(2)$ , he has shown that  $\rho$  satisfies condition (A) when  $\text{Im}(\tilde{\rho}) \cong A_4$ . The method also applies to the case  $\text{Im}(\tilde{\rho}) \cong S_4$ , at least when the quadratic field corresponding to the kernel of the composition:

$$G \xrightarrow{\tilde{\rho}} S_4 \xrightarrow{\text{sign}} \{\pm 1\}$$

is real. This approach does not appear to work in the  $A_5$  case.

Exercise: (Tate) Let  $\rho$  be a two-dimensional representation of  $G$  with odd determinant, satisfying Condition (A). Show that, for any automorphism  $\sigma$  of the field  $\mathbb{C}$ ,  $\rho^\sigma$  also satisfies (A). (Hint: use Theorems 1 and 2, and 2.5 (i).)

§4 Proof of Theorem 2

In this section, we sketch the proof of Theorem 2. For more details, see [DS].

As in the theorem, let  $f$  be a normalised newform on  $\Gamma_0(N)$  of type  $(1, \varepsilon)$ :

$$f(z) = \sum_{n=1}^{\infty} a_n q^n.$$

For a prime number  $p$ , we let  $\sigma_p$  denote a Frobenius at  $p$ . We must find a representation:

$$\rho : G \rightarrow GL_2(\mathbb{C})$$

such that, for all  $p \nmid N$ ,  $\rho$  is unramified at  $p$ , and

$$\text{Tr}(\rho(\sigma_p)) = a_p, \quad \det(\rho(\sigma_p)) = \varepsilon(p), \quad p \nmid N.$$

Here,  $\text{Tr}$  denotes the trace. Note that  $\text{Tr}(\rho(\sigma_p))$  and  $\det(\rho(\sigma_p))$  are well-defined, independent of the choice of  $\sigma_p$ , since  $\rho$  is unramified at  $p$ , for  $p \nmid N$ .

As in 2.5 above, we can find a number field  $E/\mathbb{Q}$ , of finite degree, such that the ring  $\mathcal{O}_E$  of integers of  $E$  contains all the coefficients  $a_p$ , and the values of  $\varepsilon$ . We can, moreover, assume that  $E/\mathbb{Q}$  is Galois. For each prime number  $\ell$ , let  $\mathfrak{p}_\ell$  denote a prime ideal of  $\mathcal{O}_E$  containing  $\ell$ , and let  $k_\ell = \mathcal{O}_E/\mathfrak{p}_\ell$  be the corresponding residue class field.

#### 4.1 Existence of "modular" representations:

There exists a continuous semisimple linear representation

$$\rho_\ell : G \rightarrow GL_2(k_\ell)$$

which is unramified outside  $N\ell$  and such that

$$\text{Tr}(\rho_\ell(\sigma_p)) = a_p \pmod{p_\ell}, \quad \det(\rho_\ell(\sigma_p)) = \varepsilon(p) \pmod{p_\ell}$$

for all  $p \nmid N\ell$ .

The proof relies on the following general result of Deligne [DS,6.1,6.2]:

Let  $K$  be a non-Archimedean local field, with ring of integers  $\mathcal{O}_K$ , and residual characteristic  $\ell$ . Let  $g = \sum b_n q^n$  be a modular form on  $\Gamma_0(N)$  of type  $(k, \varepsilon)$ , with  $k \geq 2$ . Assume that  $g|T_p = b_p g$  for all  $p \nmid N$ , and that  $\mathcal{O}_K$  contains these  $b_p$  and the values of  $\varepsilon$ . Then there is a semisimple continuous linear representation  $\theta_\ell : G \rightarrow GL_2(K)$  which is unramified outside  $N\ell$ , and such that:

$$\text{Tr}(\theta_\ell(\sigma_p)) = a_p, \quad \det(\theta_\ell(\sigma_p)) = p^{k-1} \varepsilon(p),$$

for all  $p \nmid N\ell$ .

Let  $m$  be an even positive integer,  $m \geq 4$ , and  $m \equiv 0 \pmod{(\ell - 1)}$ . The normalised Eisenstein series:

$$E_m = 1 - b_m^{-1} \cdot 2m \sum_{n=1}^{\infty} \sigma_{m-1}(n) q^n,$$

where  $b_m$  is the  $m$ -th Bernoulli number, is a modular form on  $\Gamma$  of weight  $m$ . It has rational  $\ell$ -integral Fourier coefficients and, as a formal power series in  $q$ :

$$E_m \equiv 1 \pmod{\ell},$$

by the Clausen-von Staudt theorem ([BS, p.384]). Hence:

$$fE_m \equiv f \pmod{p_\ell}, \quad \text{and}$$

$$fE_m|_{T_p} \equiv a_p \cdot fE_m \pmod{p_\ell}, \quad \text{for } p \nmid N.$$

The product  $fE_m$  is a modular form on  $\Gamma_0(N)$  of type  $(m+1, \epsilon)$ . By [DS 6.11], we can find a modular form  $g$  on  $\Gamma_0(N)$ , of type  $(m+1, \epsilon)$ , with  $\ell$ -integral Fourier coefficients lying in a finite extension  $E'/E$ , satisfying:

$$g|_{T_p} = b_p g, \quad \text{and} \quad b_p \equiv a_p \pmod{P_\ell},$$

for all  $p \nmid N\ell$ , and some prime  $P_\ell$  of  $E'$  dividing  $p_\ell$ . We can apply Deligne's theorem to this  $g$ , and obtain an  $\ell$ -adic representation  $\theta_\ell$  of  $G$  over the completion of  $E'$

at  $P_\ell^*$ . Replacing  $\theta_\ell$  by an isomorphic representation, if necessary, we can assume that  $\theta_\ell$  is an integral representation. So we may reduce  $\theta_\ell \bmod P_\ell$  to obtain a continuous linear representation:

$$\tilde{\rho}_\ell : G \rightarrow GL_2(k'_\ell)$$

over the residue class field  $k'_\ell/k_\ell$  at  $P_\ell$ . Further:

$$\text{Tr}(\tilde{\rho}_\ell(\sigma_p)) = a_p \pmod{P_\ell}, \quad \text{and}$$

$$\det(\tilde{\rho}_\ell(\sigma_p)) = p^m \varepsilon(p) \equiv \varepsilon(p) \pmod{P_\ell},$$

for all  $p \nmid N\ell$ .

---

\* Shimura has suggested that, instead of taking  $E_m$  as above, one uses a suitable Eisenstein series  $E_1$  of weight 1 on  $\Gamma_1(\ell)$ , in which case  $fE_1$  is of weight 2. Then one only has to use Deligne's theorem in the case  $k = 2$ , where it had been proved earlier by Eichler-Shimura-Igusa, using more elementary methods. This has the added advantage of showing that  $\rho_\ell$  appears in the natural representation of  $G$  on the  $\ell$ -division points of the Jacobian of the modular curve  $X_1(N\ell)$ , cf. Koike [K].

Let  $\rho_\ell$  be the "semisimplification" of  $\tilde{\rho}_\ell$ ; that is,  $\rho_\ell$  is a semisimple representation with the same Jordan-Hölder factors as  $\tilde{\rho}_\ell$ . We must show that  $\rho_\ell$  is realisable as a representation over  $k_\ell$ . Since the Brauer group of a finite field is trivial, it is sufficient to prove that  $\rho_\ell$  and  $\rho_\ell^\gamma$  are isomorphic, for any  $\gamma \in \text{Gal}(k'_\ell/k_\ell)$ . For a Frobenius  $\sigma_p$ ,  $p \nmid N\ell$ , we have

$$\text{Tr}(\rho_\ell(\sigma_p)) = \text{Tr}(\rho_\ell^\gamma(\sigma_p)) = a_p \pmod{P_\ell},$$

and

$$\det(\rho_\ell(\sigma_p)) = \det(\rho_\ell^\gamma(\sigma_p)) = \varepsilon(p) \pmod{P_\ell}$$

since, by hypothesis, the  $a_p$  and the values of  $\varepsilon \pmod{P_\ell}$  lie in  $k_\ell$ . The group  $\rho_\ell(G)$  is finite so that, by the Čebotarev density theorem, every element is of the form  $\rho_\ell(\sigma_p)$  for some  $p \nmid N\ell$ . Consequently,  $\rho_\ell$  and  $\rho_\ell^\gamma$  have the same characteristic polynomial, and they are isomorphic.

4.2 Exploitation of a result of Rankin: Let  $P$  denote a set of prime numbers. We define the upper density of  $P$  to be:

$$\text{upp. dens.}(P) = \lim_{\substack{s \rightarrow 1 \\ s > 1}} \sup \frac{\sum_{p \in P} p^{-s}}{\log(1/(s-1))} .$$



Let  $f, E$  be as above. Then:

For every  $\eta > 0$ , there is a finite subset  $S$  of  $\mathcal{O}_E$  such that the set  $P_S$  of primes  $p \nmid N$  with  $a_p \notin S$  has upper density  $< \eta$ .

Let  $\{\lambda_p\}$ ,  $p \nmid N$  be a system of eigenvalues of the Hecke operators  $T_p$  on  $S(\Gamma_0(N), k, \epsilon)$ . Using a result of Rankin one proves ([DS, 5.7]):

$$\sum |\lambda_p|^2 p^{-s} \leq \log(1/(s-k)) + O(1) \quad \text{as } s \rightarrow k.$$

In particular, this applies to the case  $k = 1$ ,  $\lambda_p = a_p$ , and also to  $\lambda_p = a_p^\gamma$ , for any  $\gamma \in \text{Gal}(E/\mathbb{Q})$ , (cf. 2.5). So:

$$\sum_{\gamma} \sum_{p \nmid N} |a_p^\gamma|^2 p^{-s} \leq [E:\mathbb{Q}] \cdot \log(1/(s-1)) + O(1) \quad \text{as } s \rightarrow 1,$$

where  $\gamma$  ranges over  $\text{Gal}(E/\mathbb{Q})$ . For any  $c > 0$ , the set:

$$S(c) = \{a \in \mathcal{O}_E \mid \sum_{\gamma} |a^\gamma|^2 \leq c\}$$

is finite. Consider the set  $P_{S(c)}$ . By definition, if  $p \in P_{S(c)}$ , we have:

$$\sum_{\gamma} |a_p^\gamma|^2 > c, \quad \text{so that:}$$

$$c \cdot \sum_{p \in P_{S(c)}} p^{-s} \leq [E:\mathbb{Q}] \cdot \log(1/(s-1)) + O(1) \quad \text{as } s \rightarrow 1.$$

Therefore  $\text{upp.dens.}(P_{S(c)}) \leq c^{-1}[E:\mathbb{Q}]$ , and in the assertion we may take  $S = S(\eta^{-1}[E:\mathbb{Q}])$ .

4.3 Bounds on  $\text{Im}(\rho_\ell)$ : We denote the cardinality of a finite set  $S$  by  $\#S$ . Let  $\rho_\ell$  again denote the modular representation of  $G$  over  $k$  constructed in 4.1. Let  $G_\ell = \text{Im}(\rho_\ell) \subset \text{GL}_2(k_\ell)$ , and let  $L$  denote the set of prime numbers which split completely in  $E/\mathbb{Q}$ . The set  $L$  is infinite, and for  $\ell \in L$ ,  $G_\ell \subset \text{GL}_2(\mathbb{F}_\ell)$ , where  $\mathbb{F}_\ell$  denotes the field of  $\ell$  elements. The next step is to prove

$$\sup_{\ell \in L} \#G_\ell < \infty.$$

The groups  $G_\ell$ , for  $\ell \in L$ , have the following property:  
Given  $\eta > 0$ , there exists  $M$  such that, for all  $\ell \in L$ , there is a subset  $H_\ell \subset G_\ell$ , with:

$$\#H_\ell \geq (1 - \eta) \#G_\ell, \quad \text{and}$$

$$\#\{\det(1 - ht) \in \mathbb{F}_\ell[t] \mid h \in H_\ell\} \leq M.$$

For, by 4.2 above, there is a set  $P_\eta$  of prime numbers such that:

$$(i) \quad \text{upp.dens.}(P_\eta) \leq \eta,$$

$$(ii) \quad M = \#\{a_p \mid p \notin P_\eta\} \text{ is finite.}$$

Take  $H_\ell$  to be the set of all conjugates of  $\rho_\ell(\sigma_p)$ ,  $p \notin P_\eta$ . Then  $H_\ell$  satisfies the first condition by the Chebotarev density theorem. The characteristic polynomial of  $\rho_\ell(\sigma_p)$  is  $1 - a_p t + \varepsilon(p)t^2 \pmod{p_\ell}$ . So  $H_\ell$  and  $M$  have the required properties.

A group-theoretic lemma, based on the list of subgroups of  $GL_2(\mathbb{F}_\ell)$ , applied to any  $\eta < 1/2$ , now implies the existence of a bound for  $\#G_\ell$ , cf. [DS, 7.2].

4.4 End of Proof: Since, for  $\ell$  splitting completely in  $E$ ,  $\#G_\ell$  is bounded independent of  $\ell$ ,  $\#G_\ell$  is prime to  $\ell$  for large  $\ell$ . Then, ([DS, 8.5, 8.6]), there is an integral representation  $\rho$  of  $G$ , defined over a finite extension of  $E$ , which reduces mod primes to  $\rho_\ell$ , for infinitely many  $\ell$ . Clearly, this  $\rho$  satisfies:

$\rho$  is unramified at all  $p \nmid N$ ;

$\det(\rho) = \varepsilon$ ;

$\text{Tr}(\rho(\sigma_p)) = a_p$  for all  $p \nmid N$ .

It remains, therefore, to show that:

- (i)  $\rho$  is irreducible;
- (ii)  $L(s, \rho) = L_F(s)$ ;
- (iii) the conductor of  $\rho$  is  $N$ .

Proof of (i): Suppose that  $\rho$  is reducible,  $\rho = \chi_1 \oplus \chi_2$ , say. Then  $\chi_1 \cdot \chi_2 = \epsilon$ , and  $\chi_1(p) + \chi_2(p) = a_p$  for all  $p \nmid N$ . Hence:

$$\sum |a_p|^2 p^{-s} = 2 \cdot \sum p^{-s} + \sum \chi_1(p) \cdot \bar{\chi}_2(p) p^{-s} + \sum \bar{\chi}_1(p) \cdot \chi_2(p) p^{-s}.$$

Since  $\epsilon(-1) = -1$ , the characters  $\chi_1 \bar{\chi}_2$  and  $\bar{\chi}_1 \chi_2$  are non-trivial, and so:

$$\sum \chi_1(p) \cdot \bar{\chi}_2(p) p^{-s} + \sum \bar{\chi}_1(p) \cdot \chi_2(p) p^{-s} = o(1) \quad \text{as } s \rightarrow 1.$$

Consequently:

$$\sum |a_p|^2 p^{-s} = 2 \cdot \log(1/(s-1)) + o(1), \quad \text{as } s \rightarrow 1.$$

But we know (see above):

$$\sum |a_p|^2 p^{-s} \leq \log(1/(s-1)) + o(1) \quad \text{as } s \rightarrow 1,$$

and this contradiction shows that  $\rho$  is irreducible.

Proof of (ii) and (iii): The only possible differences between  $L(s, \rho)$  and  $L_f(s)$  occur in their Euler factors at primes  $p \mid N$ . So  $\Lambda_f(s)$  and  $\Lambda(s, \rho)$  can only differ by a finite number of Euler factors and an exponential factor:

$$\Lambda(s, \rho) = \Lambda_f(s) H(s) (F(\rho) \cdot N^{-1})^{s/2}$$

and similarly

$$\Lambda(s, \bar{\rho}) = \Lambda_f(s) H'(s) (F(\rho) \cdot N^{-1})^{s/2},$$

where  $F(\rho)$  is the conductor of  $\rho$ , and  $H, H'$  are finite products of Euler factors of the form  $(1 - \alpha_p p^{-s})^{-1}$ . The functional equations of  $\Lambda_f(s)$  and  $\Lambda(s, \rho)$  imply a functional equation:

$$(F(\rho) \cdot N^{-1})^{s/2} H'(s) = c \cdot (F(\rho) \cdot N^{-1})^{(1-s)/2} H(1-s),$$

for some constant  $c \in \mathbb{C}^\times$ . Using the fact that  $|\alpha_p| < p^{\frac{1}{2}}$ , one shows easily that such an equation implies ([DS, 4.9])  $H = H' = 1$ , and  $F(\rho) = N$ .

This concludes the sketch of the proof.

## §5. Applications

One can obtain various estimates for the coefficients of a normalised newform of weight 1 on  $\Gamma_0(N)$  by using the fact that they are also the coefficients of an Artin L-series. Then one can deduce similar results for the Fourier coefficients of more general modular forms of weight 1, by reducing to newforms and Eisenstein series.

5.1 Let  $f = \sum_{n=0}^{\infty} a_n q^n$  be a non-zero modular form of type  
 $(1, \epsilon)$  on  $\Gamma_0(N)$  such that  $f|T_p = \lambda_p f$  for all  $p \nmid N$ . Then

$|\lambda_p| \leq 2$ , for all  $p \nmid N$ .

Without changing the eigenvalues  $\lambda_p$ , we may replace  $f$  by either a newform or an Eisenstein series. In the first case, Theorem 2 shows that  $\lambda_p$  is the sum of two roots of unity, and hence  $|\lambda_p| \leq 2$ . The same is true in the second case, because of Hecke's theory of Eisenstein series.

This is the Ramanujan-Petersson Conjecture in weight 1. The Conjecture is proved for weight  $\geq 2$  in [DW].

5.2 Let  $f = \sum_{n=0}^{\infty} a_n q_M^n$  be a non-zero modular form of weight 1  
on some congruence subgroup of  $SL_2(\mathbb{Z})$ . Then:

$$(a) \quad a_n = O(\sigma_0(n)) = O(n^\delta) \text{ for any } \delta > 0.$$

$$(b) \quad \limsup \frac{\log(|a_n|) \cdot \log \log n}{\log n} = \log 2.$$

$$(c) \quad \text{The set of positive integers } n \text{ for which } a_n = 0 \text{ has density 1.}$$

See [DS 9.1,9.2], [DS 9.5] and [DPP 3.5]. For newforms, (b) follows also from the following general property of Artin L-series:

Exercise: Let  $\theta$  be a  $d$ -dimensional complex linear representation of  $G$ , and let:

$$L(s, \theta) = \sum_{n=1}^{\infty} b_n n^{-s}.$$

Then:

$$\limsup \frac{\log(|b_n|) \cdot \log \log n}{\log n} = \log d.$$

5.3 The Čebotarev density theorem shows that if  $\rho^{(1)}$  and  $\rho^{(2)}$  are representations of  $G$  such that:

$$\text{Tr}(\rho^{(1)}(\sigma_p)) = \text{Tr}(\rho^{(2)}(\sigma_p))$$

for sufficiently many  $p$ , then  $\rho^{(1)}$  and  $\rho^{(2)}$  are isomorphic.

See exercises below. One can give effective forms of this in some generality ([Dur.LO]), but Theorem 1 yields a particularly sharp effective form of the Čebotarev theorem for two-dimensional representations with odd determinant:

Let  $N$  be a positive integer, and  $\epsilon$  a Dirichlet character mod  $N$ . Let  $P$  be a finite set of primes, containing all prime divisors of  $N$ . Define:

$$A(N, P, \epsilon) = N \cdot \prod_{p \in P} p^{e_p}, \quad \text{where}$$

$$e_p = \begin{cases} 2 & \text{if } p \nmid N; \\ 0 & \text{if } p^2 \mid N \text{ and } \epsilon \text{ may be defined} \\ & \text{mod } N/p \\ 1 & \text{otherwise.} \end{cases}$$



Theorem 3 Let  $\rho^{(1)}, \rho^{(2)}$  be two-dimensional complex linear representations of  $G$ , with conductor dividing  $N$ , and

$$\det(\rho^{(1)}) = \det(\rho^{(2)}) = \epsilon,$$

an odd character. Assume that  $\rho^{(1)}$  and  $\rho^{(2)}$  both satisfy condition (A) of §1, and let:

$$L(s, \rho^{(i)}) = \sum_{n=1}^{\infty} a_n^{(i)} n^{-s}, \quad \text{for } i = 1, 2.$$

Let  $P$  be a finite set of primes containing all prime divisors of  $N$ . Suppose that  $a_{\ell}^{(1)} = a_{\ell}^{(2)}$  for all primes  $\ell$  such that:

$$\ell \notin P, \quad \text{and } \ell \leq (1/12) \cdot A \cdot \prod_{p \in P} (1 + p^{-1}),$$

where  $A = A(N, P, \epsilon)$ , as above. Then:

$$\rho^{(1)} \cong \rho^{(2)}.$$

Proof: There is a constant  $a_0^{(i)}$  such that:

$$f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n, \quad \text{for } i = 1, 2,$$

is a modular form of type  $(1, \epsilon)$  on  $\Gamma_0(N)$ . (In fact,

$a_0^{(i)} = \frac{1}{2} L(0, \rho^{(i)})$ , which is zero if  $\rho^{(i)}$  is irreducible.)

Let:

$$g = f^{(1)} - f^{(2)} = \sum_{n=0}^{\infty} b_n q^n,$$

and

$$g^* = \sum_n^* b_n q^n = \sum_{n=1}^{\infty} b_n^* q^n, \quad \text{say,}$$

where  $\sum^*$  denotes the sum taken over all  $n$  prime to all  $p \in P$ .

Lemma:  $g^*$  is a modular form of type  $(1, \epsilon)$  on  $\Gamma_0(A)$ , where  $A = A(N, P, \epsilon)$ .

Fix a prime  $p$  and consider:

$$g_p = \sum_{\substack{n \\ p \nmid n}} b_n q^n.$$

Then  $g_p = g - g|U_p V_p$ , where the action of the operators  $U_p, V_p$  on power series is given by:

$$(\sum c_n q^n)|U_p = \sum c_{np} q^n, \quad \text{and} \quad (\sum c_n q^n)|V_p = \sum c_n q^{np}.$$

By the properties of these operators ([Li, p.287])  $g_p$  is a modular form of type  $(1, \epsilon)$  on  $\Gamma_0(Np^e)$ . The lemma follows by iteration.

By hypothesis, the coefficients  $b_n^*$  of  $g^*$  satisfy:

$$b_n^* = 0 \text{ for all } n \leq (1/12) \cdot A \cdot \prod_{p|A} (1 + p^{-1}).$$

If the order of  $\epsilon$  is  $r$ ,  $(g^*)^r$  is a modular form on  $\Gamma_0(A)$  of type  $(r, 1)$ , with a zero at infinity of order at least:

$$(r/12) \cdot A \cdot \prod_{p|A} (1 + p^{-1}) + r = (r/12) \cdot (\Gamma : \Gamma_0(A)) + r.$$

Consequently, by [OggA, Prop.7],  $g^*$  is identically zero, and

the result follows.

Remark: If one only assumes that  $\det(\rho^{(1)})$ ,  $\det(\rho^{(2)})$  are odd characters, not that they are equal, the theorem still holds provided  $a_\ell^{(1)} = a_\ell^{(2)}$  for all primes  $\ell \notin P$  such that:

$$\ell \leq (1/24) \cdot B^2 \cdot \prod_{p|B} (1 - p^{-2}), \quad \text{where } B = N \cdot \prod_{p \in P} p^2.$$

(Hint: work on  $\Gamma_1(N)$  rather than  $\Gamma_0(N)$ .)

### Exercises:

(i) Let  $G$  be a compact group with Haar measure  $\mu$ , and let  $\rho^{(1)}$ ,  $\rho^{(2)}$  be two  $r$ -dimensional representations of  $G$ , and suppose that the set  $A$  of  $g \in G$  such that  $\text{Tr}(\rho^{(1)}(g)) = \text{Tr}(\rho^{(2)}(g))$  satisfies  $\mu(A)/\mu(G) > 1 - 1/2r^2$ . Show that  $\rho^{(1)}$  and  $\rho^{(2)}$  are isomorphic. (Hint: use the orthogonality relations.)

(ii) Take  $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ , and show that if  $\text{Tr}(\rho^{(1)}(\sigma_p)) = \text{Tr}(\rho^{(2)}(\sigma_p))$  for all  $p$  in a set of density  $> 1 - 1/2r^2$ , then  $\rho^{(1)}$  and  $\rho^{(2)}$  are isomorphic.

(iii) Show that for  $r = 2$ , this bound is sharp (Hint: Take  $G = D_4 \times C_2$ ).

(iv) Let  $f^{(i)} = \sum_{n=1}^{\infty} a_n^{(i)} q^n$ ,  $i = 1, 2$ , be two distinct normalised newforms on  $\Gamma_0(N)$  of weight 1. Show that

the set of  $p$  for which  $a_p^{(1)} = a_p^{(2)}$  has density  $\leq 7/8$ .  
Produce an example where it is  $7/8$ .

## PART II

This part contains examples illustrating the theory of Part I, namely two-dimensional representations of  $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ , with odd determinant and the corresponding modular forms of weight 1.

We first discuss liftings of projective representations of Galois groups to linear representations (§6). We then give examples of dihedral representations (§7) and of representations (dihedral or not) which have prime conductor (§§8, 9).

Most of these results and examples were found by Tate, and communicated to Serre in a series of letters during 1973 and 1974.

## §6. Cohomology and Liftings

6.1 Let  $K$  be a global or a local field. (We assume throughout that our non-Archimedean local fields have finite residue field.) Let  $\bar{K}/K$  be a separable closure of  $K$ , and let  $G_K = \text{Gal}(\bar{K}/K)$ . Let  $\tilde{\rho}$  be a projective representation of  $G_K$ :

$$\tilde{\rho} : G_K \rightarrow \text{PGL}_n(\mathbb{C}) = \text{GL}_n(\mathbb{C})/\mathbb{C}^\times.$$

We assume throughout that all representations of  $G_K$  are continuous. A lifting of  $\tilde{\rho}$  is a (continuous) linear representation  $\rho: G_K \rightarrow \text{GL}_n(\mathbb{C})$  such that the diagram

$$\begin{array}{ccc} G_K & \xrightarrow{\rho} & \text{GL}_n(\mathbb{C}) \\ & \searrow \tilde{\rho} & \downarrow \\ & & \text{PGL}_n(\mathbb{C}) \end{array}$$

commutes. If  $\rho$  is a lifting of  $\tilde{\rho}$ , then so is  $\chi \otimes \rho$ , for any one-dimensional linear representation  $\chi$  of  $G_K$ ; further, any lifting of  $\tilde{\rho}$  is of this form, for some  $\chi$ .

We may regard  $\mathbb{C}^\times$  as a discrete  $G_K$ -module, on which  $G_K$  acts trivially. Let  $H^2(G_K, \mathbb{C}^\times)$  denote the 2-cohomology group of the profinite group  $G_K$  with coefficients in  $\mathbb{C}^\times$  (cf. [CG]). The obstruction to the existence of a lifting of  $\tilde{\rho}$  is an element of  $H^2(G_K, \mathbb{C}^\times)$ .

Theorem 4 (Tate) Let  $K$  be a local or global field. Then  
 $H^2(G_K, \mathbb{C}^\times) = 1.$

Corollary Every projective representation of  $G_K$  has a  
lifting.

We will give a proof of Theorem 4 in 6.5 below.

If  $K$  is a non-Archimedean local field, let

$P_K \subset I_K \subset G_K$  denote respectively the first ("wild") ramification group and the inertia group of  $\bar{K}/K$ . We say that a projective representation  $\tilde{\rho}$  of  $G_K$  is unramified (resp. tamely ramified) if  $\tilde{\rho}$  is trivial on  $I_K$  (resp.  $P_K$ ).

Exercise: If  $K$  is a non-Archimedean local field, an unramified (resp. tamely ramified) projective representation of  $G_K$  has an unramified (resp. tamely ramified) lifting. (Hint: Use the known structure of  $G_K/I_K$  and  $G_K/P_K$ ; cf. [CG, II-33 Ex.1].)

6.2 Now restrict to the case  $K = \mathbb{Q}$ . Let  $p$  be a prime number, and let  $I_p \subset D_p \subset G_{\mathbb{Q}}$  be respectively the inertia and decomposition groups of a place of  $\bar{\mathbb{Q}}$  above  $p$ . So  $I_p$  and  $D_p$  are uniquely determined up to conjugation, and  $D_p$  may be

identified with  $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) = G_{\mathbb{Q}_p}$ .

Theorem 5 (Tate) Let  $\tilde{\rho}$  be a projective representation of  $G_{\mathbb{Q}}$ , and for each prime number  $p$ , let  $\rho'_p$  be a lifting of  $\tilde{\rho}|_{D_p}$ . Suppose that  $\rho'_p|_{I_p}$  is trivial for almost all  $p$ . Then there is a unique lifting  $\rho$  of  $\tilde{\rho}$  such that:

$$\rho|_{I_p} = \rho'_p|_{I_p}$$

for all  $p$ .

(Note that the lifting can be specified on the inertia groups, not on the decomposition groups.)

Proof: Let  $\rho_1$  be some lifting of  $\tilde{\rho}$ . Then, for each  $p$ , we can find a one-dimensional linear representation  $\chi_p$  of  $D_p$  such that:

$$\rho'_p = \chi_p \otimes \rho_1|_{D_p}.$$

We may assume that  $\chi_p$  is unramified for almost all  $p$ . If we view  $\chi_p$  as a character of  $\mathbb{Q}_p^\times$ , there is an idele class character  $\chi$  of  $\mathbb{Q}$  such that  $\chi|_{\mathbb{Z}_p^\times} = \chi_p|_{\mathbb{Z}_p^\times}$  for all  $p$ . That is, we can find a one-dimensional linear representation  $\chi$  of  $G_{\mathbb{Q}}$  such that  $\chi|_{I_p} = \chi_p|_{I_p}$  for all  $p$ . Then  $\rho = \chi \otimes \rho_1$  is the required lifting. Since  $\rho$  is uniquely determined on



the inertia groups, it is uniquely determined.

We now define the conductor of a projective representation  $\tilde{\rho}$  of  $G_{\mathbb{Q}}$  to be the integer:

$$N = \prod_p p^{m(p)}$$

where, for each prime number  $p$ ,  $m(p)$  is the least integer such that  $\tilde{\rho}|_{D_p}$  has a lifting with conductor  $p^{m(p)}$ . Theorem 5 shows that, if  $\tilde{\rho}$  has conductor  $N$ , it has a lifting with conductor  $N$ , and every lifting has conductor a multiple of  $N$ .

6.3 Now restrict further to the case  $K = \mathbb{Q}$ ,  $n = 2$ . The groups  $\tilde{\rho}(G_{\mathbb{Q}})$ ,  $\tilde{\rho}(D_p)$  are finite subgroups of  $\mathrm{PGL}_2(\mathbb{C})$  (cf.

3.3). A lifting of  $\tilde{\rho}$  (resp.  $\tilde{\rho}|_{D_p}$ ) is reducible if and only if  $\tilde{\rho}(G_{\mathbb{Q}})$  (resp.  $\tilde{\rho}(D_p)$ ) is cyclic.

If  $\rho$  is unramified at  $p$ ,  $\tilde{\rho}(D_p)$  is necessarily cyclic, and  $m(p) = 0$ .

On the other hand, suppose that  $\tilde{\rho}$  is ramified at  $p$ , but only tamely ramified. Then  $\tilde{\rho}(D_p)$  is metacyclic, and hence is cyclic or dihedral. In the first case, any lifting of  $\tilde{\rho}|_{D_p}$  is reducible and  $m(p) = 1$ . If  $\tilde{\rho}(D_p)$  is dihedral, any lifting of  $\tilde{\rho}|_{D_p}$  is induced from a one-

dimensional representation of  $G_K$ , for some quadratic extension  $K/\mathbb{Q}_p$ . In this case,  $m(p) = 2$ .

In the wildly ramified case, with  $p \neq 2$ ,  $\tilde{\rho}(D_p)$  is still either cyclic or dihedral, since  $\tilde{\rho}(D_p)$  has a normal subgroup  $A$  which is a  $p$ -group, such that the quotient  $\tilde{\rho}(D_p)/A$  is metacyclic; one has analogous results on the conductor. In the remaining case  $p = 2$ ,  $\tilde{\rho}(D_p)$  can also be  $A_4$  or  $S_4$ , cf.  $[W_2]$ ; the exponent  $m(p)$  has been determined by J. Buhler (unpublished).

6.4 Now suppose we have a two-dimensional projective representation  $\tilde{\rho}$  of  $G_{\mathbb{Q}}$  and a Dirichlet character  $\epsilon$ . It is of some interest to know (cf. 3.3) whether  $\tilde{\rho}$  has a lifting  $\rho$  such that  $\det(\rho) = \epsilon$ . Since  $\det(\chi \otimes \rho) = \chi^2 \cdot \det(\rho)$ ,  $\tilde{\rho}$  determines the determinant of a lifting to within the square of an idele class character of  $\mathbb{Q}$ .

View  $\epsilon$  as an idele class character, and let  $\epsilon_p = \epsilon|_{\mathbb{Q}_p^\times}$ , for every place  $p$  of  $\mathbb{Q}$  (including  $\infty$ ). Define:

$$(\epsilon, p) = \epsilon_p(-1).$$

Observe that the group of characters of  $\mathbb{Q}_p^\times$  modulo squares is of order 2, so that  $(\epsilon, p) = +1$  if and only if  $\epsilon_p$  is the square of some character of  $\mathbb{Q}_p^\times$ . Also:

$$\prod_p (\epsilon, p) = +1,$$

where the product is taken over all  $p$ , including  $\infty$ .

Since  $\mathrm{PSL}_2(\mathbb{C}) = \mathrm{PGL}_2(\mathbb{C})$ , the obstruction to  $\tilde{\rho}$  having a lifting with determinant 1 is an element  $\lambda$  of  $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ . We may identify  $H^2(G_{\mathbb{Q}}, \{\pm 1\})$  with  $\mathrm{Br}_2(\mathbb{Q})$ , the subgroup of the Brauer group of  $\mathbb{Q}$  consisting of all elements  $x$  such that  $2x = 0$ . For each place  $p$  of  $\mathbb{Q}$ , the restriction  $\lambda_p$  of  $\lambda$  is an element of  $H^2(D_p, \{\pm 1\}) = \mathrm{Br}_2(\mathbb{Q}_p) \cong \{\pm 1\}$ . The element  $\lambda_p$  may also be viewed as the obstruction to  $\tilde{\rho}|_{D_p}$  having a lifting with determinant 1. We define  $(\tilde{\rho}, p)$  as the image of  $\lambda_p$  in  $\{\pm 1\}$ ; then:

$$\prod_p (\tilde{\rho}, p) = +1.$$

Theorem 6  $\tilde{\rho}$  has a lifting  $\rho$  such that  $\det(\rho) = \epsilon$  if and only if  $(\epsilon, p) = (\tilde{\rho}, p)$  for all places  $p$  of  $\mathbb{Q}$ .

(Notice that, because of the product formulas above, these statements are equivalent to  $(\epsilon, p) = (\tilde{\rho}, p)$  for all  $p$  except possibly one.)

Proof: Let  $\rho_1$  be some lifting of  $\tilde{\rho}$ . For a given  $p$ , one checks that  $(\epsilon, p) = (\tilde{\rho}, p)$  if and only if:

$$\epsilon_p \cdot \det(\rho_1)_p^{-1} = \chi_p^2,$$

for some character  $\chi_p$  of  $\mathbb{Q}_p^\times$ . This is equivalent to:

$$\epsilon_p = \det(\chi_p \otimes \rho_1|_{D_p}).$$

Suppose this holds for all  $p$ . We may assume that  $\chi_p \otimes \rho_1|_{D_p}$  is unramified for almost all  $p$ . Theorem 5 shows that there is a lifting  $\rho$  of  $\tilde{\rho}$  such that:

$$\rho|_{I_p} = \chi_p \otimes \rho_1|_{I_p}$$

for all prime numbers  $p$ . So  $\epsilon_p$  and  $\det(\rho)_p$  coincide on  $I_p$  for all prime numbers  $p$ . Hence  $\epsilon = \det(\rho)$ . The converse is now clear.

Remark: If  $c \in G_{\mathbb{Q}}$  is a Frobenius at infinity,  $\epsilon(c) = (\epsilon, \infty)$ . Also, if  $\rho$  is some lifting of  $\tilde{\rho}$ ,  $\det(\rho)$  is odd if and only if  $(\tilde{\rho}, \infty) = -1$ . So the case which will interest us is  $(\epsilon, \infty) = (\tilde{\rho}, \infty) = -1$ .

6.5 Proof of Theorem 4: The map  $x \mapsto e^{2\pi i x}$  embeds  $\mathbb{Q}/\mathbb{Z}$  in  $\mathbb{C}^\times$ , and the cokernel is uniquely divisible, so that  $H^2(G_K, \mathbb{C}^\times) = H^2(G_K, \mathbb{Q}/\mathbb{Z})$ . Hence it is enough to prove:

$$(6.5.1) \quad H^2(G_K, \mathbb{Q}/\mathbb{Z}) = 1.$$

Tate first announced (6.5.1) at the Stockholm International Congress (1962), as a consequence of deeper (and partially unproved) duality theorems(\*). The proof we give below is based on suggestions by Tate himself; for the sake of simplicity, we restrict to the characteristic zero case.

(a) Preliminary reduction

The  $p$ -primary component of  $H^2(G_K, \mathbb{Q}/\mathbb{Z})$  is  $H^2(G_K, \mathbb{Q}_p/\mathbb{Z}_p)$ , so we have to prove that  $H^2(G_K, \mathbb{Q}_p/\mathbb{Z}_p)$  vanishes for all  $p$ .

If  $E/K$  is a finite extension of degree prime to  $p$ , and  $G_E = \text{Gal}(\bar{K}/E)$ , the restriction map:

$$\text{Res}: H^2(G_K, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^2(G_E, \mathbb{Q}_p/\mathbb{Z}_p)$$

is injective ([CL, VII Prop. 6]). Consequently, it is enough to prove that  $H^2(G_K, \mathbb{Q}_p/\mathbb{Z}_p)$  vanishes when  $K$  contains the group  $\mu_p$  of  $p$ -th roots of unity.

Since  $H^2(G_K, \mathbb{Q}_p/\mathbb{Z}_p)$  is  $p$ -torsion, it is sufficient to prove that multiplication by  $p$  is injective. That is, we have to show that the coboundary map:

$$\delta: H^1(G_K, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^2(G_K, \mathbb{Z}/p\mathbb{Z})$$

---

\*

One of them is known to be equivalent to the still unproved "Leopoldt's Conjecture" on the non-vanishing of the  $p$ -adic regulator.

in the cohomology sequence attached to

$$0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p \rightarrow 0,$$

is surjective.

Since we are assuming that  $K$  contains the group  $\mu_p$  of  $p$ -th roots of unity, we may identify  $H^2(G_K, \mathbb{Z}/p\mathbb{Z})$  with  $H^2(G_K, \mu_p) = \text{Br}_p(K)$ , the subgroup of the Brauer group of  $K$  consisting of all elements  $x$  such that  $px = 0$ .

(b) Local case (see also [CG,p.II-25] and [SS,p.232])

The case when  $K$  is Archimedean is trivial. So we may assume that  $K$  is a non-Archimedean local field, and, as in (a), that it contains the  $p$ -th roots of unity. So  $\text{Br}_p(K) = \mathbb{Z}/p\mathbb{Z}$ , and it is enough to prove that  $\delta \neq 0$ .

The group  $H^1(G_K, \mathbb{Q}_p/\mathbb{Z}_p)$  is just the group of continuous homomorphisms  $G_K \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ , and, via class field theory, this group may in turn be identified with the group of continuous homomorphisms  $\phi: K^\times \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ . Now,  $\delta(\phi) = 0$  if and only if  $\phi$  is a  $p$ -th power, and the known structure of  $K^\times$  shows that  $\phi$  is a  $p$ -th power if and only if  $\phi$  is trivial on  $\mu_p$ . There certainly exist continuous homomorphisms  $K^\times \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$  which are non-trivial on  $\mu_p$ , and so  $\delta$  is non-zero, as required.

(The case of non-zero characteristic is slightly



different, but easier.)

(c) Global case

Now assume that  $K$  is an algebraic number field containing

$\mu_p$ . We have to show that:

$$\delta: H^1(G_K, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow \text{Br}_p(K)$$

is surjective.

Let  $J_K$  denote the idele group of  $K$ ,  $C_K = J_K/K^\times$  the idele class group of  $K$ , and  $D_K$  the connected component of  $C_K$ . Then, via class field theory, we may identify  $H^1(G_K, \mathbb{Q}_p/\mathbb{Z}_p)$  with the group of continuous homomorphisms  $C_K/D_K \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ .

An element  $\alpha \in \text{Br}_p(K)$  is described by its local components  $\alpha_v \in \text{Br}_p(K_v)$  for all places  $v$  of  $K$ . If we view the  $\alpha_v$  as elements of  $\mathbb{Z}/p\mathbb{Z}$ , we have:

(i)  $\alpha_v = 0$  for almost all  $v$ ;

(ii)  $\alpha_v = 0$  if  $v$  is complex, or if  $v$  is real and  $p \neq 2$ ;

(iii)  $\sum_v \alpha_v = 0$ .

Given  $\alpha \in \text{Br}_p(K)$ , there exist continuous homomorphisms  $\chi_v: K_v^\times \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$  such that  $\delta(\chi_v) = \alpha_v$ , for all places  $v$  of  $K$ , by the local theory. Further, the image  $\delta(\chi_v)$  depends



only on  $\phi_v$ , the restriction of  $\chi_v$  to the group  $\mu_{p,v}$  of  $p$ -th roots of unity in  $K_v$ . If we can construct a continuous homomorphism  $\phi: J_K \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ , factoring through  $J_K \rightarrow C_K/D_K$ , such that  $\phi|_{\mu_{p,v}} = \phi_v$  for all places  $v$  of  $K$ , then  $\delta(\phi) = \alpha$ . Moreover, by (iii) above, it will be sufficient to verify that  $\phi|_{\mu_{p,v}} = \phi_v$  for all  $v$  except possibly one.

Fix a non-Archimedean place  $v_0$  of  $K$ , and define:

$$\mu_J = \prod_{v \neq v_0} \mu_{p,v} \subset J_K.$$

The  $\phi_v$  determine a continuous homomorphism  $\phi_J: \mu_J \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$  which, we assert, is trivial on the kernel  $\mu_X$  of the composition:

$$\mu_J \rightarrow J_K \rightarrow C_K \rightarrow C_K/D_K.$$

Now,  $\mu_J \cap K^\times = \{1\}$ , so  $\mu_J$  embeds in  $C_K$ . We must determine  $\mu_J \cap D_K$ . But, ([AT,p.90]),  $D_K$  is the product of  $\mathbb{R}$ , a "solenoid", and  $(\mathbb{R}/\mathbb{Z})^{r_2}$  where  $r_2$  is the number of complex places of  $K$ . The solenoid is the Pontrjagin dual of the discrete group  $\mathbb{Q}^{r_1+r_2-1}$ , where  $r_1$  is the number of real places of  $K$ . The solenoid and  $\mathbb{R}$  are torsion free, so  $\mu_X$  is a subgroup of  $(\mathbb{Z}/p\mathbb{Z})^{r_2}$ . But  $\mu_X$  clearly contains  $\mu_{p,v}$  if  $v$  is complex, so:

$$\mu_X = \prod_{\substack{v \\ \text{complex}}} \mu_{p,v}.$$

The map  $\phi_J$  is clearly trivial on this group.

So  $\phi_J$  defines a continuous homomorphism  $\bar{\mu}_J \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ , where  $\bar{\mu}_J$  denotes the image of  $\mu_J$  in  $C_K/D_K$ . Since  $\mu_J$  is compact,  $\bar{\mu}_J$  is closed, and  $\phi_J$  extends to a homomorphism  $\phi: C_K/D_K \rightarrow \mathbb{R}/\mathbb{Z}$ . But  $C_K/D_K$  is totally disconnected, so the image of  $\phi$  is a finite subgroup of  $\mathbb{Q}/\mathbb{Z}$ . Consequently, the extension  $\phi$  may be chosen to take values in  $\mathbb{Q}_p/\mathbb{Z}_p$ , and we have  $\delta(\phi) = \alpha$ . Therefore,  $\delta$  is surjective, as required.

This argument also applies in non-zero characteristic; that case is easier, since  $D_K = \{1\}$ .

## §7. Dihedral Representations

7.1 Let  $\tilde{\rho}$  be a two-dimensional projective linear representation of  $G_{\mathbb{Q}}$ , and let  $\rho$  be some lifting of  $\tilde{\rho}$ . We say that  $\tilde{\rho}$  (or  $\rho$ ) is dihedral if  $\tilde{\rho}(G_{\mathbb{Q}}) \subset \mathrm{PGL}_2(\mathbb{C})$  is isomorphic to the dihedral group  $D_n$  of order  $2n$ , for some  $n \geq 2$ . A dihedral representation is irreducible.

Let  $C_n$  be a cyclic subgroup of  $D_n$  of order  $n$ ; if  $n \geq 3$ ,  $C_n$  is uniquely determined. If  $\tilde{\rho}$  is a dihedral representation, the composition

$$\omega : G_{\mathbb{Q}} \xrightarrow{\tilde{\rho}} D_n \longrightarrow D_n/C_n = \{\pm 1\}$$

is a one-dimensional linear representation of  $G_{\mathbb{Q}}$  of order 2, corresponding to some quadratic extension  $K/\mathbb{Q}$ . If  $G_K = \text{Gal}(\bar{\mathbb{Q}}/K) \subset G_{\mathbb{Q}}$ , then  $\tilde{\rho}(G_K) = C_n$ , and  $\rho|_{G_K}$  is reducible:

$$\rho|_{G_K} = \chi \oplus \chi',$$

say, for some one-dimensional representations  $\chi, \chi'$  of  $G_K$ . If  $\sigma$  lies in the non-identity coset of  $G_{\mathbb{Q}}/G_K$ , then  $\chi' = \chi_{\sigma}$ , where  $\chi_{\sigma}(\gamma) = \chi(\sigma\gamma\sigma^{-1})$ ,  $\gamma \in G_K$ . Further,  $\rho = \text{Ind}_{K/\mathbb{Q}}(\chi)$ , the representation of  $G_{\mathbb{Q}}$  induced by  $\chi$ .

7.2 Suppose, conversely, that we start with a quadratic number field  $K/\mathbb{Q}$ , corresponding to a character  $\omega$  of  $G_{\mathbb{Q}}$ , and a one-dimensional linear representation  $\chi$  of  $G_K$ . Let  $\rho = \text{Ind}_{K/\mathbb{Q}}(\chi)$ , and let  $\tilde{\rho}$  be the associated projective representation of  $G_{\mathbb{Q}}$ . If  $\sigma$  generates  $\text{Gal}(K/\mathbb{Q})$ , let  $\chi_{\sigma}$  be as above. Let  $f$  be the conductor of  $\chi$ , and  $d_K$  the discriminant of  $K/\mathbb{Q}$ .

(7.2.1) With the above notations:

- (a) The following are equivalent: (i)  $\rho$  is irreducible; (ii)  $\rho$  is dihedral; (iii)  $\chi \neq \chi_{\sigma}$ .
- (b) The conductor of  $\rho$  is  $|d_K| \cdot N_{K/\mathbb{Q}}(f)$ .
- (c) The representation  $\det(\rho)$  of  $G_{\mathbb{Q}}$  is odd if and

only if either:

(i)  $K$  is imaginary,

or

(ii)  $K$  is real and  $\chi$  has signature  $+, -$  at infinity; that is, if  $c, c' \in G_K$  are Frobenius elements at the two real places of  $K$ , then  
 $\chi(c) \neq \chi(c')$ .

(d) If  $\tilde{\rho}(G_{\mathbb{Q}}) = D_n$ , then  $n$  is the order of  $\chi^{-1} \cdot \chi_{\sigma}$ .

Proof: (a)  $\rho|_{G_K}$  is reducible, so  $\tilde{\rho}(G_K)$  is cyclic. Therefore  $\tilde{\rho}(G_{\mathbb{Q}})$  has a cyclic subgroup of index  $\geq 2$ , and from the list of finite subgroups of  $\mathrm{PGL}_2(\mathbb{C})$ , one sees that  $\tilde{\rho}(G_{\mathbb{Q}})$  must be either cyclic or dihedral. The equivalence of (i) and (ii) is now clear. The equivalence of (i) and (iii) follows immediately from [SRL, Prop.22].

(b) is the standard conductor formula for induced representations, as in [Dur.M].

(c) The representation  $\det(\rho)$  is given by ([Dur.M, 3,2]):

$$\det(\rho) = \omega \chi_{\mathbb{Q}},$$

where  $\chi_{\mathbb{Q}}$  is the representation  $\chi \circ \mathrm{ver}_{K/\mathbb{Q}}$  of  $G_{\mathbb{Q}}$ ,

$\mathrm{ver}_{K/\mathbb{Q}}: G_{\mathbb{Q}}/(G_{\mathbb{Q}}, G_{\mathbb{Q}}) \rightarrow G_K/(G_K, G_K)$  being the transfer map. As

idele class character,  $\chi_{\mathbb{Q}}$  is just the restriction of  $\chi$  to the idele class group of  $\mathbb{Q}$ . The character  $\omega$  is odd if and only if  $K$  is imaginary. If  $K$  is imaginary, and  $v$  is the Archimedean place of  $K$ ,  $\chi|_{K_v^\times}$  is necessarily trivial, so  $\chi_{\mathbb{Q}}$  is even.

Suppose, on the other hand, that  $K$  is real. Then  $\omega$  is even, and  $\det(\rho)$  is odd if and only if  $\chi_{\mathbb{Q}}$  is odd. This, in turn, is equivalent to  $\chi$  having signature  $+, -$ .

(d)  $C_n$  is the image  $\tilde{\rho}(G_K)$ . Up to similarity,  $\rho|_{G_K}$  is the representation:

$$\gamma \mapsto \begin{pmatrix} \chi(\gamma) & 0 \\ 0 & \chi_{\sigma}(\gamma) \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & \chi^{-1} \chi_{\sigma}(\gamma) \end{pmatrix} \pmod{\mathbb{C}^\times} \subset GL_2(\mathbb{C}).$$

So  $n$  is the order of  $\chi^{-1} \cdot \chi_{\sigma}$ .

Remark: If we view  $\chi$  as a ray class character mod  $\mathfrak{f}$  of  $K$ , then  $\chi$  has signature  $+, -$  if and only if  $\chi(x\sigma_K) = -1$ , for any totally positive  $x \in K$  such that  $x \equiv -1 \pmod{\mathfrak{f}^\times}$ . Indeed, a real quadratic field  $K$  has a character with conductor  $\mathfrak{f}$  and signature  $+, -$  if and only if  $K$  has no totally positive unit  $u$  such that  $u \equiv -1 \pmod{\mathfrak{f}^\times}$ . In particular, a character  $\chi$  with signature  $+, -$  has conductor  $\mathfrak{f}$  such that

$N_{K/\mathbb{Q}}(\mathfrak{f}) > 1$ . So a dihedral representation with odd determinant attached to a real quadratic field cannot have prime conductor.

7.3 If  $\rho = \text{Ind}_{K/\mathbb{Q}}(\chi)$  is a dihedral representation of  $G_{\mathbb{Q}}$ , it satisfies Condition (A) of §1. Hence, if  $\epsilon = \det(\rho)$  is odd, and we put:

$$L(s, \rho) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad f(z) = \sum_{n=1}^{\infty} a_n q^n,$$

then, by Theorem 1,  $f(z)$  is a cusp form on  $\Gamma_0(N)$  of type  $(1, \epsilon)$ , where  $N = |d_K| \cdot N_{K/\mathbb{Q}}(\mathfrak{f})$ , in the above notation. The cusp form  $f$  is a linear combination of  $\theta$ -series of binary quadratic forms attached to  $K$  (cf. [H,23]).

For example, take  $K$  imaginary and  $\chi$  unramified. View  $\chi$  as a character of the ideal class group of  $\mathcal{O}_K$ . For any ideal  $a$  of  $\mathcal{O}_K$ ,  $a \cdot \sigma(a)$  is principal, so  $\chi \neq \chi_{\sigma}$  if and only if  $\chi^2 \neq 1$ . Therefore an imaginary quadratic field  $K$  gives rise to a dihedral representation of  $G_{\mathbb{Q}}$  of this type if its ideal class group is not an elementary abelian 2-group. The smallest value of  $|d_K|$  for which this happens is 23.

The class number of  $\mathbb{Q}(\sqrt{-23})$  is 3; the Hilbert class field  $H$  of  $\mathbb{Q}(\sqrt{-23})$  is generated by the roots of  $X^3 - X - 1 = 0$ ,



and  $\text{Gal}(H/\mathbb{Q}) \cong D_3$ . If  $\rho$  is the irreducible two-dimensional linear representation of  $\text{Gal}(H/\mathbb{Q})$ , then:

$$L(s, \rho) = L_f(s),$$

where

$$f = \frac{1}{2}(\theta_1 - \theta_2),$$

and

$$\theta_1 = \sum_{m,n \in \mathbb{Z}} q^{m^2 + mn + 6n^2}, \quad \theta_2 = \sum_{m,n \in \mathbb{Z}} q^{2m^2 + mn + 3n^2};$$

$\theta_1, \theta_2$  are the  $\theta$ -series of the two classes of primitive binary quadratic forms over  $\mathbb{Z}$  with discriminant  $-23$ .

Further:

$$f = q \cdot \prod_{n=1}^{\infty} (1 - q^n) (1 - q^{23n}) = \eta(z)\eta(23z),$$

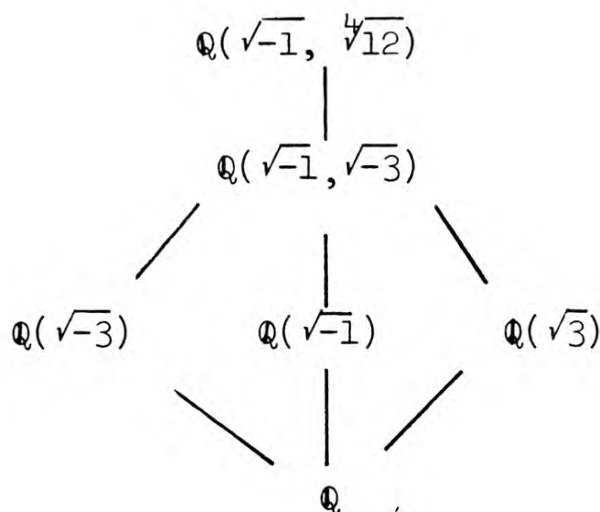
where  $\eta$  is Dedekind's  $\eta$ -function.

Similarly,  $\mathbb{Q}(\sqrt{-31})$  has class number 3; its Hilbert class field  $H$  is generated by the roots of  $X^3 + X - 1 = 0$ , and  $\text{Gal}(H/\mathbb{Q}) \cong D_3$ . The irreducible two-dimensional linear representation of  $\text{Gal}(H/\mathbb{Q})$  corresponds to the cusp form:

$$f = \frac{1}{2} \left( \sum q^{m^2 + mn + 8n^2} - \sum q^{2m^2 + mn + 4n^2} \right).$$

A different kind of example is given by the extension  $E/\mathbb{Q}$ , where  $E = \mathbb{Q}(\sqrt{-1}, \sqrt[4]{12})$ , cf. [H, 22, 23, pp. 425, 426, 448]:





We have  $\text{Gal}(E/\mathbb{Q}) \cong D_4$ . The modular form associated to the irreducible two-dimensional linear representation  $\rho$  of  $\text{Gal}(E/\mathbb{Q})$  is:

$$f(z) = \sum (-1)^n \cdot q^{m^2+n^2}$$

where the sum is taken over all pairs  $(m,n) \in \mathbb{Z} \times \mathbb{Z}$  such that:

$$m \equiv 1 \pmod{3}, \quad n \equiv 0 \pmod{3}, \quad m+n \equiv 1 \pmod{2}.$$

One has:

$$f(z) = q \cdot \prod_{n=1}^{\infty} (1 - q^{12n})^2 = \eta(12z)^2.$$

The conductor of  $\rho$  is 144. The image of  $\tilde{\rho}$  in  $\text{PGL}_2(\mathbb{C})$  is  $D_2$ . The group  $D_2$  has three distinct cyclic subgroups  $C_2$ , corresponding to the three quadratic subfields of  $E$ . Each of these gives a presentation of  $\rho$  as an induced

representation, and hence an expression for  $f$  in terms of theta-series of the associated quadratic field. For instance  $\mathbb{Q}(\sqrt{-1})$  gives the expression  $\sum (-1)^n q^{m^2+n^2}$  above.

## §8. Representations with Prime Conductor

We now consider irreducible two-dimensional linear representations  $\rho: G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$  with odd determinant, and prime conductor  $p$ .

### 8.1 Classification (after a letter of Tate, dated March 26th, 1974)

I) Dihedral Case: Suppose that  $\rho$  is dihedral, in the sense of §7. If  $\rho$  has conductor  $p$ , it follows from 7.2.1 and 7.3 that:

$$(i) \quad p \equiv 3 \pmod{4}.$$

(ii)  $\rho = \text{Ind}_{K/\mathbb{Q}}(\chi)$ , where  $K = \mathbb{Q}(\sqrt{-p})$ , and  $\chi$  is an unramified character of  $K$  such that  $\chi^2 \neq 1$ .

(iii) The character  $\varepsilon = \det(\rho)$  is the Legendre symbol  $n \mapsto \left(\frac{n}{p}\right)$ .

Such a representation does indeed correspond to a form on  $\Gamma_0(p)$ , namely  $\sum_a \chi(a) \cdot q^{Na}$ , where the sum is taken over all integral ideals  $a$  of the ring  $\mathcal{O}_K$  of integers of  $K$ .

If  $p \equiv 3 \pmod{4}$  and  $h$  is the class number of  $\mathbb{Q}(\sqrt{-p})$ , then  $h$  is odd ([BS, p.346, Th.3]), and there are precisely  $(h-1)/2$  non-isomorphic dihedral representations with conductor  $p$ .

Exercise: Show that every irreducible two-dimensional representation of  $G_{\mathbb{Q}}$  has conductor  $\geq 23$ . (Hint: use Odlyzko [Dur.0] combined with tables of cubic and quartic fields.)

II) Non-dihedral Case: Recall that, if  $\rho$  is irreducible and not dihedral, then  $\tilde{\rho}(G_{\mathbb{Q}}) \subset \mathrm{PGL}_2(\mathbb{C})$  is isomorphic to either  $A_4$ ,  $S_4$ , or  $A_5$ .

Theorem 7 Let  $\rho$  be an irreducible two-dimensional linear representation of  $G_{\mathbb{Q}}$  with prime conductor  $p$  such that  $\varepsilon = \det(\rho)$  is odd. Assume that  $\rho$  is not dihedral. Then:

- (a)  $p \not\equiv 1 \pmod{8}$ ;
- (b) if  $p \equiv 5 \pmod{8}$ ,  $\rho$  is of type  $S_4$  (i.e.  $\tilde{\rho}(G_{\mathbb{Q}}) \cong S_4$ ) and  $\varepsilon$  is of order 4 and conductor  $p$ ;
- (c) if  $p \equiv 3 \pmod{4}$ ,  $\rho$  is of type  $S_4$  or  $A_5$ , and  $\varepsilon$  is the Legendre symbol  $n \mapsto \left(\frac{n}{p}\right)$ .

Proof: The conductor of  $\varepsilon$  divides  $p$ . Since  $\varepsilon$  is odd,  $\varepsilon \neq 1$ , so the conductor of  $\varepsilon$  is precisely  $p$ . If  $I_p$  is the inertia group of a place of  $\bar{\mathbb{Q}}$  above  $p$ ,  $\rho|_{I_p} = \psi \oplus 1$ , for some one-dimensional representation  $\psi \neq 1$  of  $I_p$ , since the conductor of  $\rho$  is  $p$ . It follows that the canonical homomorphisms

$$\rho(I_p) \rightarrow \varepsilon(I_p) \quad \text{and} \quad \rho(I_p) \rightarrow \tilde{\rho}(I_p)$$

are isomorphisms. Since  $\varepsilon$  is ramified only at  $p$ , we have  $\varepsilon(I_p) = \varepsilon(G_{\mathbb{Q}})$ , and this group is cyclic of even order. So  $\tilde{\rho}(I_p)$  is a cyclic subgroup of even order of  $A_4$ ,  $S_4$  or  $A_5$ . Therefore this order is 2 or 4, and  $\varepsilon$  is of order 2 or 4.

On the other hand, since  $\varepsilon$  is a character with conductor  $p$ , we may view it as a character of  $(\mathbb{Z}/p\mathbb{Z})^\times$ ; since  $\varepsilon(-1) = -1$ ,  $\varepsilon$  is faithful on the 2-primary component of  $(\mathbb{Z}/p\mathbb{Z})^\times$ . So, if  $p \equiv 1 \pmod{8}$ , the order of  $\varepsilon$  is  $\geq 8$ , which is impossible. If  $p \equiv 5 \pmod{8}$ ,  $\varepsilon$  is of order 4, and since  $A_4$  and  $A_5$  have no elements of order 4,  $\rho$  is of type  $S_4$ .

Suppose now that  $p \equiv 3 \pmod{4}$ . Then  $\varepsilon$  is of order 2, and must therefore be the Legendre symbol. If  $\rho$  were of type  $A_4$ , the image of  $I_p$  under the composition:

$$I_p \xrightarrow{\tilde{\rho}} A_4 \longrightarrow C_3$$

would be trivial. Then the kernel of the composition  $G_{\mathbb{Q}} \rightarrow A_4 \rightarrow C_3$  would correspond to an everywhere unramified cubic field. This is impossible, so  $\rho$  is of type  $S_4$  or  $A_5$ .

Corollary If  $p \equiv 1 \pmod{8}$ , every cusp form of weight 1 on  $\Gamma_1(p)$  is zero.

Conversely, start with a Galois extension  $E/\mathbb{Q}$ , and a prime number  $p$ . Consider the following three cases:

(b)  $\text{Gal}(E/\mathbb{Q}) \cong S_4$  and  $p \equiv 5 \pmod{8}$ ;

(c<sub>1</sub>)  $\text{Gal}(E/\mathbb{Q}) \cong S_4$  and  $p \equiv 3 \pmod{4}$ ;

(c<sub>2</sub>)  $\text{Gal}(E/\mathbb{Q}) \cong A_5$  and  $p \equiv 3 \pmod{4}$ .

An embedding of  $\text{Gal}(E/\mathbb{Q})$  in  $\text{PGL}_2(\mathbb{C})$  defines a projective representation  $\tilde{\rho}_E$  of  $G_{\mathbb{Q}}$ . Notice that in cases (b) and (c<sub>1</sub>),  $\tilde{\rho}_E$  is essentially unique, since any two embeddings of  $S_4$  in  $\text{PGL}_2(\mathbb{C})$  are conjugate, while in case (c<sub>2</sub>), there are two conjugacy classes of embeddings of  $A_5$  in  $\text{PGL}_2(\mathbb{C})$ .

Theorem 8  $\tilde{\rho}_E$  has a lifting with conductor  $p$  and odd determinant if and only if:

Case (b):  $E$  is the normal closure of a non-real quartic field  $E_4/\mathbb{Q}$  with discriminant  $p^3$ ;

Case ( $c_1$ ):  $E$  is the normal closure of a quartic field  
 $E_4/\mathbb{Q}$  with discriminant  $-p$ ;

Case ( $c_2$ ):  $E$  is the normal closure of a non-real  
quintic field  $E_5/\mathbb{Q}$  with discriminant  $p^2$ .

When these conditions are satisfied, in each case  $\tilde{\rho}_E$   
has precisely two non-isomorphic liftings with odd deter-  
minant and conductor  $p$ ; if one of these is  $\rho$ , the other  
is  $\bar{\rho} = \rho \otimes \varepsilon$ , where  $\varepsilon = \det(\rho)$ .

Proof: We only prove the sufficiency of these conditions;  
the necessity follows readily from Theorem 7.

Lemma: Let  $\tilde{\rho}$  be any two-dimensional projective represent-  
ation of  $G_{\mathbb{Q}}$ , and  $p$  any prime number. Let  $i_p = \# \tilde{\rho}(I_p)$ .  
Assume that  $i_p$  is prime to  $p$  (i.e.,  $\tilde{\rho}$  is tamely ramified  
at  $p$ ) and  $i_p \geq 3$ . Then the conductor of  $\tilde{\rho}$  is exactly  
divisible by  $p$  if and only if  $i_p \mid (p-1)$ .

Since  $\tilde{\rho}$  is tamely ramified,  $\tilde{\rho}(D_p)$  is either cyclic or  
dihedral. The conductor of  $\tilde{\rho}$  is exactly divisible by  $p$  if  
and only if  $\tilde{\rho}(D_p)$  is cyclic (6.3). But  $\tilde{\rho}(I_p)$  is cyclic,  
and contains an element of order  $\geq 3$ , so  $\tilde{\rho}(D_p)$  is cyclic  
if and only if it is abelian. Now, the group  $\tilde{\rho}(D_p)/\tilde{\rho}(I_p)$



is cyclic, generated by an element  $F$  such that  $FxF^{-1} = x^p$ , for all  $x \in \tilde{\rho}(I_p)$ . So  $\tilde{\rho}(D_p)$  is abelian if and only if  $i_p | (p-1)$ .

In Case (b) of the Theorem, the condition  $p \equiv 5 \pmod{8}$  implies that  $p$  is tamely ramified in  $E$ , and hence that  $\tilde{\rho}_E$  is tamely ramified at  $p$ . The discriminant condition on  $E_4$  implies that the ramification index of  $p$  in  $E$  is at least 4. So  $\tilde{\rho}_E(I_p)$  is cyclic of order 4, and the result follows from the Lemma and Theorem 5.

Now consider the cases  $(c_1), (c_2)$  of the Theorem. If  $\epsilon$  is the Legendre symbol,  $(\epsilon, \infty) = -1$ . Also,  $(\tilde{\rho}_E, \infty) = -1$ . If  $\ell$  is a prime,  $\ell \neq p$ , then  $(\epsilon, \ell) = +1$ . One verifies directly that an unramified (local) projective representation has a lifting with determinant 1, so  $(\tilde{\rho}_E, \ell) = +1$  also. By Theorem 6,  $\tilde{\rho}_E$  has a lifting  $\rho$  such that  $\det(\rho) = \epsilon$ . It is easy to see that  $\rho$  may be chosen to be unramified outside  $p$ . Observe that there are precisely two choices for  $\rho|_{I_p}$ .

The conductor of  $\rho$  is a power of  $p$ . We show it is precisely  $p$ . Since  $\rho$  is tamely ramified,  $\rho(I_p)$  is cyclic, generated by some matrix which we may take to be of the form:

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$



Now  $\det(\rho) = \varepsilon$ , so  $ab = -1$ . On the other hand,  $\tilde{\rho}_E(I_p)$  has order 2, so  $a = -b$ , and either  $a$  or  $b$  is equal to 1; hence  $\rho$  has conductor  $p$ .

The uniqueness statement is now immediate.

One can also determine the images  $\rho(G_{\mathbb{Q}})$  for the representations  $\rho$  given by Theorem 8. One finds that  $\rho(G_{\mathbb{Q}})$  consists of all elements  $s \in GL_2(\mathbb{C})$  whose image  $\tilde{s}$  in  $PGL_2(\mathbb{C})$  lies in  $\tilde{\rho}_E(G_{\mathbb{Q}})$  such that:

$$(b) \quad \det(s)^2 = \text{sgn}(\tilde{s}) \quad (\text{where } \text{sgn}: S_4 \rightarrow \{\pm 1\});$$

$$(c_1) \quad \det(s) = \text{sgn}(\tilde{s});$$

$$(c_2) \quad \det(s) = \pm 1.$$

The orders of these groups are respectively 96, 48 and 240.

The fields of values of the character of  $\rho$  are respectively  $\mathbb{Q}(\sqrt{-1})$ ,  $\mathbb{Q}(\sqrt{-2})$  and  $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ .

**8.2 Numerical Examples:** We use the notation and list of cases of Theorem 8.

Case (b):  $p \equiv 5 \pmod{8}$

The group  $S_3$  is a quotient of  $S_4$ , so  $E$  contains a totally real cubic subfield with discriminant  $p$ . Hence 3 divides the class number of  $\mathbb{Q}(\sqrt{p})$ , and the tables of class

numbers of quadratic fields (e.g. [BS]) show that the only  $p < 1000$  with this property are  $p = 229$  and  $p = 733$ .

For  $p = 229$ , Tate has constructed a representation of type  $S_4$  with conductor 229: if  $x_1, x_2, x_3$  are the roots of  $X^3 - 4X + 1 = 0$ , the field generated by the  $\sqrt{-3 + 8x_1}$  has Galois group  $S_4$ , and gives a representation  $\rho_1$  of the required type. One can also take the field generated by the  $\sqrt{4 - 3x_1^2}$ ; this gives a representation  $\rho_2$  which is not isomorphic to  $\rho_1$  or  $\bar{\rho}_1$ . Langlands' theorem (see [LB] and 3.3) shows that  $\rho_1$  and  $\rho_2$  correspond to modular forms  $f_1, f_2$ , say. If we choose  $\rho_1$  and  $\rho_2$  (from among their conjugates) so that  $\det(\rho_1) = \det(\rho_2) = \epsilon$ , where  $\epsilon$  is the character of order 4 of  $(\mathbb{Z}/229\mathbb{Z})^\times$  such that  $\epsilon(2) = i$ , the first coefficients of  $f_1, f_2$  are (H.Cohen):

$$f_1 = q + q^3 - iq^4 + iq^5 + (i-1)q^7 - iq^{11} - iq^{12} + \dots$$

$$f_2 = q + (1+i)q^2 - q^3 + iq^4 + iq^5 - (1+i)q^6 + \dots$$

These are both newforms on  $\Gamma_0(229)$  of type  $(1, \epsilon)$ , and one may show (see 9.3) that  $f_1, f_2, \bar{f}_1, \bar{f}_2$  are the only newforms on  $\Gamma_0(229)$  of weight 1.

Case  $(c_1)$ :  $p \equiv 3 \pmod{4}$ , type  $S_4$

The tables in [G] show that the only primes  $p < 1000$

for which there are quartic fields with discriminant  $-p$  are 283, 331, 491, 563, 643, 751. (These tables list all such fields for  $p < 3280$ .) One thus gets representations; it is not (yet) known whether they satisfy Condition (A), i.e. whether they correspond to modular forms of weight 1.

Case ( $c_2$ ):  $p \equiv 3 \pmod{4}$ , type  $A_5$

There are no adequate tables of quintic fields.

Computations done by J. Buhler suggest that there are no representations of this type with  $p < 1000$ .

#### §9. Modular Forms of Weight One on $\Gamma_0(p)$

This section is a continuation of §8 from the point of view of modular forms. If  $p$  is a prime and  $f = \sum a_n q^n$  is a normalised newform on  $\Gamma_0(p)$  of weight 1, then Theorem 2 shows that there is an irreducible two-dimensional linear representation  $\rho$  of  $G_{\mathbb{Q}}$ , whose conductor is  $p$ , such that  $L(s, \rho) = \sum_{n=1}^{\infty} a_n n^{-s}$ . The character of  $f$  is  $\det(\rho)$ , and  $\rho$  satisfies Condition (A) of §1. We say that  $f$  is of dihedral type (resp. type  $S_4$ , type  $A_5$ ) if  $\rho$  is of dihedral type (resp. type  $S_4$ , type  $A_5$ ), in the terminology of §8. Recall that Theorem 7 shows that  $A_4$  cannot arise.

9.1 A Bound on the Number of Representations: Suppose  $p \equiv 3 \pmod{4}$ ,  $p \neq 3$ ; we are therefore in cases  $(c_1)$ ,  $(c_2)$  of §8. Let  $\omega$  be the Legendre symbol:

$$\omega(n) = \left( \frac{n}{p} \right).$$

There is a unique reducible two-dimensional linear representation of  $G_{\mathbb{Q}}$  with conductor  $p$  and determinant  $\omega$ , namely  $1 \oplus \omega$ . This representation corresponds to the Eisenstein series:

$$G_{\omega} = \frac{1}{2} L(-1, \omega) + \sum_{n=1}^{\infty} \left( \sum_{\substack{d|n \\ d>0}} \omega(d) \right) q^n.$$

One has  $L(-1, \omega) = h$ , the class number of  $\mathbb{Q}(\sqrt{-p})$ , and this is an odd integer ([BS, p.346]).

If  $\epsilon$  is any Dirichlet character mod  $p$ , it follows from Theorem 7 that the space  $S(\Gamma_0(p), 1, \epsilon)$  of cusp forms on  $\Gamma_0(p)$  of type  $(1, \epsilon)$  is null unless  $\epsilon = \omega$ . The space  $S(\Gamma_0(p), 1, \omega)$  has a basis of normalised newforms, consisting of:

$\frac{1}{2}(h - 1)$  forms of dihedral type,

$2s$  forms of type  $S_4$ ,

$4a$  forms of type  $A_5$ ,

where  $s$  (resp.  $a$ ) is the number of quartic (resp. quintic) fields  $E/\mathbb{Q}$  satisfying the hypotheses of Theorem 8 Case  $(c_1)$

(resp.  $(c_2)$ ) whose associated representations satisfy Condition (A). So:

$$\dim S(\Gamma_0(p), 1, \omega) = \frac{1}{2}(h - 1) + 2s + 4a.$$

We now give an upper bound for  $2s + 4a$ :

Theorem 9 (i) If  $p$  is of the form  $24m - 1$  or  $24m + 7$ , then either

$$2s + 4a \leq m - (h - 1), \quad \text{or} \quad s = a = 0.$$

(ii) If  $p$  is of the form  $24m + 11$  or  $24m + 19$ , then either:

$$2s + 4a \leq m - \frac{3}{2}(h - 1), \quad \text{or} \quad s = a = 0.$$

Proof: Let  $W = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ . If  $f \in M(\Gamma_0(p), 1, \omega)$ , we have  $f|_1 W \in M(\Gamma_0(p), 1, \bar{\omega})$ . Since  $\bar{\omega} = \omega$ , this shows that  $f \mapsto f|_1 W$  is an endomorphism of  $M(\Gamma_0(p), 1, \omega)$ . Moreover, we have  $f|_1 W^2 = -f$ , hence the eigenvalues of  $W$  acting on  $M(\Gamma_0(p), 1, \omega)$  are  $\pm i$ .

(9.1.1) (i) If  $f \in M(\Gamma_0(p), 1, \omega)$  is either the Eisenstein series  $G_\omega$  or a newform of dihedral type, we have  $f|_1 W = -if$ .  
 (ii) If  $f$  is a newform of type  $S_4$  or  $A_5$ , the vector space spanned by  $f$  and  $\bar{f}$  is two-dimensional; it is stable

under  $W$ , and the eigenvalues of  $W$  on this space are  $i$  and  $-i$ .

(Recall that if  $f = \sum a_n q^n$ , we put  $\bar{f} = \sum \bar{a}_n q^n$ .) Set  $f' = f|_1 W$ . One knows (cf. 2.4) that  $f' = cf$ , and  $\Lambda_f(1-s) = ic\Lambda_{\bar{f}}(s)$  for some constant  $c$ . In case (i), the coefficients of  $f$  are real, so  $f = \bar{f}$ . It is easy to show that the representation  $\rho$  corresponding to  $f$  is realisable over  $\mathbb{R}$ . So, by a theorem of Fröhlich-Queyrut [Dur.T],  $\Lambda(1-s, \rho) = \Lambda(s, \rho)$ . Hence  $ic = 1$ , and  $c = -i$ , which proves (i).

In case (ii), it follows from Theorem 8 that  $f$  and  $\bar{f}$  are linearly independent. We have  $f|_1 W = c\bar{f}$ ,  $\bar{f}|_1 W = c'f$ , so that  $f$  and  $\bar{f}$  span a space stable under  $W$ , and the action of  $W$  on this space is given by the matrix  $\begin{pmatrix} 0 & c' \\ c & 0 \end{pmatrix}$ . This has trace 0, so that both  $i$  and  $-i$  are eigenvalues of  $W$ .

Remark: In case (i) of 9.1.1, the fact  $c = -i$  can also be deduced from the transformation formulae for theta-functions; cf. [H,23].

(9.1.2) Let  $M_+$  (resp.  $M_-$ ) denote the space of modular forms

of type  $(1, \omega)$  on  $\Gamma_0(p)$  such that  $f|_1 W = \text{if}$  (resp.  $-\text{if}$ ).

Then:

$$\dim M_+ = 1 + \frac{1}{2}(h - 1) + s + 2a,$$

and

$$\dim M_- = s + 2a.$$

Moreover,  $M_-$  is contained in the space of cusp forms

$S(\Gamma_0(p), 1, \omega).$

This follows from 9.1.1.

To prove the Theorem, we must find a bound for  $\dim(M_-)$ . If  $f \in M_+$ ,  $g \in M_-$ , then  $F = fg$  is a cusp form of type (2.1) on  $\Gamma_0(p)$  such that  $F|_2 W = F$ . Write  $\Omega_+$  for the space of such forms. The dimension  $g_+$  of  $\Omega_+$  is the genus of the curve  $X_0^*(p)$  which is the quotient of  $X_0(p)$  by the involution:

$$W: z \mapsto -1/pz.$$

This genus is determined by Fricke in [F, vol.2, p.366]; in the notation of the Theorem:

$$g_+ = \begin{cases} m - \frac{1}{2}(h - 1) & \text{in case (i)} \\ m - (h - 1) & \text{in case (ii)} \end{cases}.$$

We now use the following lemma (well-known in the theory of "linear systems"):



Lemma: Let  $L, M, N$  be non-zero finite-dimensional vector spaces over an algebraically closed field. Let  $B: L \times M \rightarrow N$  be a bilinear map such that  $B(x,y) = 0$  implies either  $x = 0$  or  $y = 0$ . Then:

$$\dim(L) + \dim(M) \leq \dim(N) + 1.$$

(Proof: Let  $H$  be the kernel of the linear map  $L \otimes M \rightarrow N$  defined by  $B$ . We have  $\text{codim}(H) \leq \dim(N)$ . Let  $X$  be the cone of  $L \otimes M$  consisting of all elements  $x \otimes y$  with  $x \in L, y \in M$ . Then  $X$  is an irreducible algebraic variety whose dimension is  $\dim(L) + \dim(M) - 1$ . By assumption, we have  $H \cap X = \{0\}$ , hence  $\dim(H \cap X) = 0$ . But an elementary result from algebraic geometry shows that  $\dim(H \cap X) \geq \dim(X) - \text{codim}(H)$ , and the lemma follows.)

We apply the lemma to the bilinear map  $(f,g) \mapsto fg$  of  $M_+ \times M_-$  into  $\Omega_+$ . Under the assumption that  $M_+$  and  $M_-$  are non-zero (i.e.  $a \neq 0$  or  $s \neq 0$ ), we get:

$$(1 + \frac{1}{2}(h-1) + s + 2a) + (s + 2a) \leq g_+ + 1,$$

i.e.

$$2s + 4a \leq g_+ - \frac{1}{2}(h-1) = \begin{cases} m - (h-1) & \text{in case (i)} \\ m - \frac{3}{2}(h-1) & \text{in case (ii),} \end{cases}$$

which proves the Theorem.

Numerical Examples: Write  $A(p)$  for the upper bound for  $2s + 4a$  given by Theorem 9. It is easy to tabulate  $A$ . If  $A(p) < 2$ , one has  $s = a = 0$ , and so all normalised newforms of weight 1 on  $\Gamma_0(p)$  are of dihedral type. If  $p < 300$ , one finds  $A < 2$  except in the following cases:

$p$	$m$	$h$	$A(p)$
139	5	3	2
163	6	1	6
211	8	3	5
227	9	5	3
283	11	3	8

The cases  $p = 139$  and  $p = 227$  are easy to deal with; as  $A(p) < 4$ , the only possibility, apart from  $a = s = 0$ , is  $s = 1$ ,  $a = 0$ . This is impossible since the tables in [G] show there are no quartic fields with discriminant  $-p$ . The same method applies to  $p = 163$  and  $p = 211$ , once one knows  $a = 0$ . One can prove this using reduction mod  $p$ , as in 9.3 below, but it is simpler to use the following result:

(9.1.3) If  $p$  is a prime for which  $a \neq 0$ , there is an extension  $K/\mathbb{Q}$ , of degree  $N = 240$ , whose discriminant  $d_K$

satisfies  $|d_K|^{1/N} = \sqrt{p}$ .

Proof: By hypothesis, there is a representation  $\rho: G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$  of type  $A_5$  with conductor  $p$ . Take  $K$  to be the field corresponding to the kernel of  $\rho$ . The degree  $[K:\mathbb{Q}]$  is 240, as in 8.1. Since  $K/\mathbb{Q}$  is ramified only at  $p$ , and the inertia group is of order 2, one has the result.

The lower bounds for  $|d_K|^{1/N}$  obtained by Odlyzko ([Dur.0]) show  $\sqrt{p} > 16.28$ , hence  $p > 265$ , which excludes  $p = 163$  and  $p = 211$ . (A more recent variation of this method gives  $p > 350$ , and even  $p > 500$  under the generalised Riemann Hypothesis.)

In the case  $p = 283$ , [G] shows that  $s \leq 1$ , with equality if the Artin Conjecture holds, and  $a = 0$  by (9.1.3).

Remark: As  $p \rightarrow \infty$ , the bound for  $2s + 4a$  given by Theorem 9 is of the form:

$$2s + 4a \leq \frac{p}{24} - O(p^{\frac{1}{2}+\epsilon}), \text{ for any } \epsilon > 0.$$

It seems likely that  $2s + 4a$  is  $O(p^\alpha)$  for some  $\alpha < 1$  (maybe even  $\alpha < \frac{1}{2}$ ), but we do not know how to prove this.

9.2 The Case  $p \equiv -1 \pmod{24}$ : Now take  $p \equiv -1 \pmod{24}$ .

In this case, we define an element  $g$  of  $M_-$  as follows.

Consider the two primitive binary quadratic forms with discriminant  $-p$  which represent 6:

$$Q(x,y) = 6x^2 + xy + \frac{p+1}{24} y^2; \quad Q'(x,y) = 6x^2 + 5xy + \frac{p+25}{24} y^2.$$

Let

$$\theta = \sum_{x,y \in \mathbb{Z}} q^{Q(x,y)}, \quad \theta' = \sum_{x,y \in \mathbb{Z}} q^{Q'(x,y)}$$

be the corresponding  $\theta$ -functions, and let:

$$g = \frac{1}{2}(\theta - \theta') = q^m(1 - q - q^2 + \dots), \quad \text{where } m = \frac{p+1}{24}.$$

Then  $g \in M_-$ , and:

$$g(z) = \eta(z) \eta(pz) = q^m \prod_{n=1}^{\infty} (1 - q^n)(1 - q^{pn}),$$

where  $\eta$  is the Dedekind  $\eta$ -function (cf. [Sch <sub>$\theta$</sub> ]).

(9.2.1) The map  $f \mapsto fg$  is an isomorphism of the space  $M_+$  onto the subspace  $\Omega_+(m)$  of  $\Omega_+$  consisting of all forms  $F$  whose Fourier expansion at infinity is divisible by  $q^{m+1}$  (or, equivalently,  $q^m$ ).

(Recall that  $\Omega_+$  is the space of cusp forms of weight 2

on  $\Gamma_0(p)$  which are invariant under  $W:z \mapsto -1/pz$ .)

This follows immediately from the observation that  $g$  does not vanish anywhere on the upper half-plane.

If  $F \in \Omega_+$ ,  $F(z)dz$  is a differential form of the first kind on the curve  $X_0^*(p)$ , and  $\Omega_+(m)$  may thus be identified with the space of differential forms of the first kind on  $X_0^*(p)$  with a zero of order at least  $m$  at the cusp. Since  $\dim(M_+) = \dim(\Omega_+(m)) = s + 2a$ , this gives a "geometrical" interpretation of the quantity  $s + 2a$ .

The genus  $g_+$  of  $X_0^*(p)$  is  $m - (h - 1)/2$ , and so  $g_+ \leq m$ .

One concludes:

(9.2.2) If  $p = 24m - 1$ , we have  $s + 2a \neq 0$  if and only if infinity is a Weierstrass point with gap  $\gamma \geq (h - 1)/2$  of the curve  $X_0^*(p)$ .

In his Durham lecture (not in this volume; but see [A]), Atkin explained how one can compute the gap  $\gamma_p$  of the reduction of  $X_0^*(p) \bmod p$ . One has  $\gamma \leq \gamma_p$ , and it would be interesting to know whether there is equality. Atkin has found  $\gamma_p < (h - 1)/2$  for  $p < 1823$ , and this is sufficient to prove  $s = a = 0$  in these cases. On the other hand, for

$p = 1823$ , Atkin has found  $\gamma_p = (h - 1)/2$ , in perfect accord with the fact that there does exist a quartic field with discriminant  $-1823$  ([G]).

9.3 Reduction modulo  $p$ : We now exploit the results of [Sp] to give a bound on the dimension of the space of modular forms of weight 1 on  $\Gamma_0(p)$ . One knows ([Sp. §3]) that every modular form on  $\Gamma_0(p)$  is congruent, modulo  $p$ , to a modular form on  $SL_2(\mathbb{Z})$ .

a) The case  $p \equiv 3 \pmod{4}$

We retain the notations of 9.1. Let  $K/\mathbb{Q}$  be a number field whose ring of integers  $\mathcal{O}_K$  contains all the Fourier coefficients of the normalised newforms  $f_1, f_2, \dots, f_r$  of type  $(1, \omega)$  on  $\Gamma_0(p)$  (cf. 2.5). Let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_K$  dividing  $p$ . Let  $F = \mathcal{O}_K/\mathfrak{p}$ ; then  $F$  is a finite extension of  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , and the  $f_i$  define, by reduction modulo  $\mathfrak{p}$ , forms  $\tilde{f}_i$  with coefficients in  $F$ .

(9.3.1) The forms  $\tilde{f}_i$  are cusp forms (in characteristic  $p$ ) of weight  $(p + 1)/2$  on  $SL_2(\mathbb{Z})$ , and they are linearly independent.

Using Th.12 of [Sp,3.4] one sees that  $\tilde{f}_i$  is a cusp form on  $SL_2(\mathbb{Z})$  of weight congruent to  $(p+1)/2$  modulo  $(p-1)$ . Let  $\rho_i$  be the representation of  $G_{\mathbb{Q}}$  which corresponds to  $f_i$ . Since the conductor of  $\rho_i$  is  $p$ , the  $p$ -factor of  $L(s, \rho_i)$  is  $(1 - u_i p^{-s})^{-1}$ , for some root of unity  $u_i$ . So  $f_i|U_p = u_i f_i$ , and  $\tilde{f}_i|U_p = \tilde{u}_i \tilde{f}_i$ , where  $\tilde{u}_i$  is the image of  $u_i$  in  $F$ . Since  $\tilde{u}_i \neq 0$ , it follows from Theorem 6 of [Sp,2.2] that the filtration  $w(\tilde{f}_i)$  of  $\tilde{f}_i$  is  $\leq (p+1)$ . Using the congruence  $w(\tilde{f}_i) \equiv (p+1)/2 \pmod{(p-1)}$ , we then see that  $w(\tilde{f}_i) = (p+1)/2$ , which proves the first part of (9.3.1).

Moreover, the images of the  $\rho_i$ 's are finite groups of order prime to  $p$ ; hence the  $\rho_i$ 's remain mutually non-isomorphic after reduction modulo  $p$ , and this implies the linear independence of the  $\tilde{f}_i$ .

The  $f_i$  have the following properties:

- (1) If  $\ell \neq p$  is a prime,  $f_i|T_\ell = a_{\ell,i} f_i$ .
- (2) If  $f_i$  is of dihedral type,  $a_{\ell,i} = 0$  for all  $\ell$  such that  $\omega(\ell) = -1$ .
- (3) If  $f_i$  is of type  $S_4$ ,  $\omega(\ell) a_{\ell,i}^2 = 0, 1, 2$ , or  $4$ .
- (4) If  $f_i$  is of type  $A_5$ ,  $\omega(\ell) a_{\ell,i}^2 = 0, 1, 4$ , or  $(3 \pm \sqrt{5})/2$ .



The  $\tilde{f}_i$  have the same properties. One can now obtain a bound on the number  $r$  of  $f_i$ 's by proceeding as follows. One writes down a basis for the space of cusp forms (mod  $p$ ) of weight  $(p+1)/2$  on  $SL_2(\mathbb{Z})$ , and finds the normalised eigenfunctions of the Hecke operators  $T_\ell$  and  $U_p$ . One eliminates those whose  $p$ -th coefficient  $a_p$  is zero, and those with a coefficient  $a_\ell$  not satisfying properties (2) - (4). The number of eigenfunctions remaining is then  $\geq r$ .

Exercise: Let  $v$  be the dimension of the space of cusp forms  $f = \sum a_n q^n$  of weight  $(p+1)/2$  on  $SL_2(\mathbb{Z})$  with coefficients in  $\mathbb{F}_p$  such that  $a_n = 0$  whenever  $\omega(n) \neq +1$ . Show that  $s + 2a \leq v$ . (For  $p = 163$ , H. Cohen has shown that  $v = 0$ , and hence that  $s = a = 0$ .)

b) The case  $p \equiv 5 \pmod{8}$

Here one is interested in forms on  $\Gamma_0(p)$  of type  $(1, \epsilon)$ , where  $\epsilon$  is a character of order 4 of  $(\mathbb{Z}/p\mathbb{Z})^\times$  (cf. §8).

Choose  $K$  and  $p$ , as in a), with the extra condition:

$$\epsilon(n) \equiv n^{(p-1)/4} \pmod{p} \text{ for all } n.$$

If  $f_1, \dots, f_s$  are the normalised newforms on  $\Gamma_0(p)$  of type  $(1, \epsilon)$ , let  $\tilde{f}_1, \dots, \tilde{f}_s$  be their reductions modulo  $p$ . Then:

(9.3.2) The  $\tilde{f}_i$  are cusp forms (in characteristic  $p$ ) of weight  $(p + 3)/4$  on  $SL_2(\mathbb{Z})$  and they are linearly independent.

The proof is analogous to that of (9.3.1).

One has a precisely similar method for obtaining an upper bound for the number  $s$  of newforms. In particular, for  $p = 229$ , one has  $(p + 3)/4 = 58$ , and the space of cusp forms of this weight has dimension 4. H. Cohen has shown that there are at most two functions  $f_i$ , namely:

$$f_1 \equiv \Delta \cdot (84E_6^7E_4 + 30E_6^5E_4^4 + 128E_6^3E_4^7 + 217E_6E_4^{10}) \pmod{229}$$

$$f_2 \equiv -\Delta(30E_6^7E_4 + 133E_6^5E_4^4 + 99E_6^3E_4^7 + 195E_6E_4^{10}) \pmod{229},$$

where  $E_4, E_6$  are the normalised (i.e. having constant term

1) Eisenstein series on  $SL_2(\mathbb{Z})$  of weights 4, 6 respectively. In fact, both of these functions do occur, because of Langlands' theorem [LB]; cf. 8.2.

#### REFERENCES

- [A] A.O.L. Atkin, Modular forms of weight one and super-singular equations (unpublished abstract - A.M.S. meeting, 1975).

- [AT] E.Artin & J.Tate, Class Field Theory (Benjamin, New York, 1967).
- [BS] Z. Borevich & I. Shafarevich, Number Theory (Academic Press, London, 1966).
- [CL] J-P.Serre, Corps Locaux (Hermann, Paris, 2nd ed., 1968).
- [CG] J-P.Serre, Cohomologie Galoisienne (Springer Lecture Notes vol. 5, 4th ed., 1973).
- [DA] P.Deligne, Formes modulaires et représentations de  $GL(2)$  (Springer Lecture Notes vol. 349. 1973, 55-105).
- [DPP] J-P.Serre, Divisibilité de certaines fonctions arithmétiques (Séminaire Delange-Pisot-Poitou, 1974/75, no. 20). To appear in Ens. Math.
- [DS] P.Deligne & J-P.Serre, Formes modulaires de poids 1 (Ann. sci. E.N.S. 4<sup>e</sup> ser., t.7, 1974, 507-530).
- [DW] P.Deligne, La conjecture de Weil I (Publ. Math. I.H.E.S. vol.43, 1974, 273-307).
- [F] R.Fricke, Die elliptischen Funktionen und ihre Anwendungen, 2 vol. (Teubner-Verlag, Leipzig-Berlin, 1922; Johnson Reprint Corp., New York, 1972).
- [G] H.J.Godwin, On quartic fields of signature one with small discriminant (Quart. Jl. Math. (Oxon.) (2), 8, 1957, 214-222).
- [H,22] E.Hecke, Über einen neuen Zusammenhang zwischen Modulfunktionen und indefiniten quadratischen Formen (no.22 in "Mathematische Werke", Vandenhoeck & Ruprecht, Göttingen, 1970 (2nd ed.)).
- [H,23] E.Hecke, Zur Theorie der elliptischen Modulfunktionen, (no.23 in "Werke").

- [H,24] E.Hecke, Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik (no.24 in "Werke").
- [H,36] E.Hecke, Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung II (no. 36 in "Werke").
- [J-L] H.Jacquet & R.Langlands, Automorphic forms on  $GL(2)$  (Springer Lecture Notes vol. 114, 1970).
- [K] M.Koike, Congruences between cusp forms of weight one and of weight two and a remark on a theorem of Deligne and Serre (Int. Symposium on Alg. Number Theory, Kyoto, March 1976).
- [LB] R.Langlands, Base change for  $GL(2)$  (Lecture notes, I.A.S. Princeton, 1975).
- [Li] W.Li, Newforms and functional equations (Math. Ann. 212, 1975, 285-315).
- [Ogg] A.Ogg, Modular Forms and Dirichlet Series (Benjamin, New York, 1969).
- [OggA] A.Ogg, Survey of modular functions of one variable (Springer Lecture Notes vol. 320, 1973, 1-36).
- [P] H.Petersson, Über die systematische Bedeutung der Eisensteinschen Reihen (Abh. Math. Sem. Univ. Hamburg 16, 1949, 104-126).
- [Sch] B.Schoeneberg, Elliptic Modular Functions (Springer-Verlag, Grundle. Math. Wiss. vol.203, 1974).
- [Sch<sub>0</sub>] B.Schoeneberg, Bemerkungen über einige Klassen von Modulfunktionen (Neder. Akad. W. Proc., A, 70, 1967, 177-182).
- [Sh] G.Shimura, Introduction to the Arithmetic Theory of Automorphic Functions (Princeton University Press, 1971).

- [Sp] J-P.Serre, Formes modulaires et fonctions zêta p-  
adiques (Springer Lecture Notes vol. 350, 1973,  
191-268).
- [SRL] J-P.Serre, Représentations Linéaires des Groupes  
Finis (Hermann, Paris, 1971 (2nd ed.)).
- [SS] S.S.Shatz, Profinite Groups, Arithmetic, and  
Geometry (Ann. Math. Studies vol. 70, Princeton  
1972).
- [W] A.Weil, Über die Bestimmung Dirichletscher Reihen  
durch Funktionalgleichungen (Math. Ann. 168,  
1967, 149-156).
- [W<sub>2</sub>] A.Weil, Exercices dyadiques (Inv. Math. 27, 1974,  
1-22).
- [WL] A.Weil, Dirichlet Series and Automorphic Forms  
(Springer Lecture Notes vol. 189, 1971).

This volume:

- [Dur.LO] J.C.Lagarias & A.Odlyzko, Effective versions of  
the Cebotarev density theorem.
- [Dur.M] J.Martinet, Character theory and Artin L-  
functions.
- [Dur.O] A.Odlyzko, On conductors and discriminants.
- [Dur.T] J.Tate, Local constants.

# p-adic L-functions and Iwasawa's theory

John Coates

## Introduction

These lectures give the still largely conjectural description of a certain Iwasawa module attached to a totally real number field  $F$  in terms of the abelian p-adic L-functions of  $F$ , together with some related material. This subject is the fusion of two rather different developments in number theory. One was the introduction by Iwasawa of his  $\Gamma$ -modules attached to  $\mathbb{Z}_p$ -extensions, and his study of them by classical class field theory. The other was Leopoldt and Kubota's construction of the abelian p-adic L-functions of  $\mathbb{Q}$ . In recent years, this latter work has been extended to all totally real number fields by Serre, Deligne and Ribet, and others. The key idea of relating the two (in the case  $F = \mathbb{Q}$ ) via Stickelberger's classical theorem is due to Iwasawa, and the underlying ideas of these lectures depend heavily on his work. The actual



choice of the material covered (and much of this is only done sketchily) has been made with two points in mind. Firstly, we work throughout with an arbitrary totally real base field  $F$  rather than  $F = \mathbb{Q}$ , at the cost of introducing still more conjectures. Secondly, we give only those aspects of the theory which are directly relevant to the connexion between  $p$ -adic  $L$ -functions and  $\Gamma$ -modules. Thus many important topics have been omitted (e.g. Iwasawa's bilinear form, and the techniques used to construct  $p$ -adic  $L$ -functions). On the other hand, Stickelberger's theorem, which is so essential to the connexion, has been treated in some detail. There would be great interest in finding precise analogues of the conjectures discussed here for non-cyclotomic  $\mathbb{Z}_p$ -extensions of certain non-totally real fields (e.g. imaginary quadratic fields). In fact, for imaginary quadratic base fields, important work on the construction of  $p$ -adic  $L$ -functions has already been done by Katz, Lichtenbaum, and Manin-Vishik, but the connexion with  $\Gamma$ -modules is still lacking. In conclusion, I wish to heartily thank R. Greenberg, S. Lichtenbaum, and W. Sinnott for many helpful discussions on the material of these lectures.



## CONTENTS

- §1. The algebraic theory
  - 1.1. Class field theory
  - 1.2. Basic Iwasawa module
  - 1.3. Kummer theory
  - 1.4. p-adic residue formula
- §2. Stickelberger ideals
  - 2.1. Partial zeta functions
  - 2.2. Norm congruence lemma
  - 2.3. Integrality
  - 2.4. Stickelberger ideals
- §3. Stickelberger's theorem
  - 3.1. Gauss sums
  - 3.2. Proof of Stickelberger's theorem
- §4. p-adic L-functions
  - 4.1. Values of L-functions
  - 4.2. Construction of the  $G(T, \chi)$
  - 4.3. p-adic L-functions
- §5. The main conjecture
  - 5.1. The main conjecture
  - 5.2. Non group-theoretic evidence for  
the main conjecture

- 5.3. Group-theoretic evidence for  
the main conjecture
- 5.4. Proof of the main conjecture  
in special cases
- 5.5 Consequences of the main  
conjecture

## Appendix 1

### §1. The algebraic theory

Let  $F$  be a finite extension of  $\mathbb{Q}$ ,  $p$  a prime number, and  $F_\infty$  the field obtained by adjoining to  $F$  all  $p$ -power roots of unity. In this section, we define a certain  $p$ -adic representation, which we denote by  $X_\infty$ , of the Galois group of  $F_\infty$  over  $F$ . The rest of these lectures will then be devoted to the study of this representation. In §1, we use only methods from class field theory and commutative algebra to study  $X_\infty$  (for this reason, we call this part the algebraic theory). The underlying idea, due principally to Iwasawa, is to view  $X_\infty$  as a module over the ring  $\Lambda$  of formal power series in an indeterminate  $T$  with coefficients in  $\mathbb{Z}_p$ . Class field theory shows that  $X_\infty$  is finitely generated over  $\Lambda$ , and it enables us to find the  $\Lambda$ -rank of

$X_\infty$  modulo  $\Lambda$ -torsion. However, as far as is known at present, these algebraic methods alone tell us very little about the  $\Lambda$ -torsion submodule  $t(X_\infty)$  of  $X_\infty$ . In the remainder of the lectures, we assume that  $F$  is totally real, and give what is still a largely conjectural description of the part of  $t(X_\infty)$ , which is fixed by complex conjugation, in terms of  $p$ -adic  $L$ -functions.

Throughout,  $r_1, r_2$  will denote the number of real and complex primes of  $F$ , respectively; also  $S$  will denote the set of primes of  $F$  lying above  $p$ . By a  $p$ -extension of a number field, we mean a Galois extension whose Galois group is a projective limit of finite  $p$ -groups. If  $H/K$  is a Galois extension of fields, we write  $G(H/K)$  for the Galois group of  $H$  over  $K$ . The rank of a finitely generated  $\mathbb{Z}_p$ -module will always mean the rank of  $Y$  modulo torsion. If  $V$  is a finite set,  $\#(V)$  will denote the cardinality of  $V$ . Finally, we denote the algebraic closure of the field of  $p$ -adic numbers  $\mathbb{Q}_p$  by  $\mathbb{C}_p$ , and we always suppose that the valuation  $|\cdot|_p$  of  $\mathbb{C}_p$  is normalized so that  $|p|_p = p^{-1}$ .

### 1.1. Class field theory

We recall the main facts from class field theory used

in §1. Let  $L$  be the maximal unramified abelian  $p$ -extension of  $F$ , and  $M$  the maximal abelian  $p$ -extension of  $F$  which is unramified outside  $S$  ( $=$  set of primes above  $p$ ). By class field theory,  $G(L/F)$  is isomorphic via the Artin map to the  $p$ -primary subgroup of the ideal class group of  $F$ . Let  $E$  be the global units of  $F$ . For each  $p \in S$ , let  $U_p$  be the units of the completion of  $F$  at  $p$ , and let

$$\phi : E \rightarrow \prod_{p \in S} U_p$$

be the diagonal map. Write  $U_{p,1}$  for the local units  $\equiv 1 \pmod{p}$ , and  $E_1$  for the global units  $\equiv 1 \pmod{p}$  for each  $p \in S$ .

Theorem 1.1.  $G(M/L)$  is isomorphic via the Artin map to  $(\prod_{p \in S} U_{p,1}) / \overline{\phi(E_1)}$ , where the bar denotes closure in the  $p$ -adic topology.

Corollary 1.2.  $G(M/F)$  is a finitely generated  $\mathbb{Z}_p$ -module, and its rank is equal to  $r_2 + 1 + \delta$ , where  $\delta = \mathbb{Z}$ -rank of  $E - \mathbb{Z}_p$ -rank of  $\overline{\phi(E_1)}$ .

Leopoldt has conjectured that  $\delta = 0$  always. At present,

this is only known (see [1]) for  $F$  abelian either over  $\mathbb{Q}$  or over an imaginary quadratic field.

## 1.2. The basic Iwasawa module

A  $\mathbb{Z}_p$ -extension of  $F$  is a Galois extension  $F_\infty/F$  whose Galois group is topologically isomorphic to the additive group of the ring  $\mathbb{Z}_p$  of  $p$ -adic integers. This is the same as saying that there is a unique tower of fields

$$F = F_0 \subset F_1 \subset \dots \subset F_n \subset \dots \subset F_\infty = \bigcup_{n \geq 0} F_n, \quad ,$$

such that each  $F_n$  is cyclic over  $F$  of degree  $p^n$ . In these lectures, we shall only be concerned with the so called cyclotomic  $\mathbb{Z}_p$ -extension of  $F$ . By definition, this is the unique  $\mathbb{Z}_p$ -extension of  $F$  contained in the field  $F_\infty = F(W)$ , where  $W$  is the group of all  $p$ -power roots of unity.

Let  $F_\infty/F$  be an arbitrary  $\mathbb{Z}_p$ -extension (we postpone for the moment the assumption that it is the cyclotomic one).

Suppose we are given an extension  $N_\infty$  of  $F_\infty$  satisfying

(i)  $N_\infty/F_\infty$  is an abelian  $p$ -extension, and (ii)  $N_\infty/F$  is Galois (but not necessarily abelian). Put

$$X_\infty = G(N_\infty/F_\infty), \quad G_\infty = G(N_\infty/F), \quad \Gamma = G(F_\infty/F),$$

so that  $G_\infty/X_\infty = \Gamma$ . Since  $X_\infty$  is abelian,  $\Gamma$  operates on  $X_\infty$

via inner automorphisms in the usual way. Namely, if  $\gamma \in \Gamma$ , we pick a representative  $u_\gamma$  of  $\gamma$  in  $G_\infty$ , and define  $\gamma \circ x = u_\gamma x u_\gamma^{-1}$  for all  $x \in X_\infty$ . Thus  $X_\infty$  is a compact continuous  $\Gamma$ -module. Moreover,  $X_\infty$ , being a profinite abelian  $p$ -group, is a  $\mathbb{Z}_p$ -module in the obvious way. Let  $\Lambda$  be the ring of formal power series in an indeterminate  $T$  with coefficients in  $\mathbb{Z}_p$ . Choose a fixed topological generator  $\gamma_0$  of  $\Gamma$ . Then the  $\Gamma$  and  $\mathbb{Z}_p$ -module structures on  $X_\infty$  give rise to a unique  $\Lambda$ -module structure on  $X_\infty$  satisfying (i) the  $\mathbb{Z}_p$ -action is the same, and (ii)  $(1 + T)x = \gamma_0$  for all  $x \in X_\infty$  (see [19]). The following lemma enables us to use class field theory to study  $X_\infty$ , by relating certain quotients of  $X_\infty$  to the finite layers  $F_n$  ( $n \geq 0$ ) of  $F_\infty/F$ . Let  $\omega_n = (1 + T)^{p^n} - 1$ .

Lemma 1.3. For each  $n \geq 0$ , let  $N_n$  be the maximal abelian extension of  $F_n$  contained in  $N_\infty$ . Then  $G(N_n/F_\infty) = X_\infty/\omega_n X_\infty$ .

Proof. By the definition of  $N_n$ ,  $G(N_\infty/N_n)$  is the closure in  $G_\infty$  of the commutator subgroup of  $G(N_\infty/F_n)$ . Choose  $h \in G(N_\infty/F_n)$  whose restriction to  $F_\infty$  is  $\gamma_0^{p^n}$ . Since  $G(F_\infty/F_n)$  is topologically generated by  $\gamma_0^{p^n}$ , it follows

that  $G(N_\infty/F_n)$  is topologically generated by  $h$  and  $X_\infty$ . But, for  $x \in X_\infty$ ,

$$hxh^{-1}x^{-1} = \gamma_0^{p^n} x - x = \omega_n x.$$

Hence the closure of the commutator subgroup of  $G(N_\infty/F_n)$  must be  $\omega_n X_\infty$ , as required.

Corollary 1.4.  $X_\infty$  is finitely generated over  $\Lambda$  if and only if  $G(N_\infty/F_\infty)$  is a finitely generated  $\mathbb{Z}_p$ -module.

Proof. It is well known that  $X_\infty$  is finitely generated over  $\Lambda$  if and only if  $X_\infty/m X_\infty$  is finite, where  $m = (p, T)$  is the maximal ideal of  $\Lambda$ . But

$$X_\infty/m X_\infty = X_0/pX_0, \quad \text{where} \quad X_0 = X_\infty/\omega_n X_\infty.$$

Clearly  $X_0/pX_0$  is finite if and only if  $X_0$  is finitely generated over  $\mathbb{Z}_p$ , and so the corollary follows from Lemma 1.3.

Before making a particular choice of the extension  $N_\infty$  of  $F_\infty$ , we note the following basic fact, which follows easily from the theory of higher ramification.



Lemma 1.5. A  $\mathbb{Z}_p$ -extension  $F_\infty/F$  is unramified outside  $S$  (= set of primes above  $p$ ).

We now take  $N_\infty$  to be the maximal abelian  $p$ -extension of  $F_\infty$ , which is unramified outside the primes of  $F_\infty$  lying above  $p$ . Also, from now on, we follow tradition and write  $M_\infty$  rather than  $N_\infty$  for this field. Let  $M_n$  be the maximal abelian  $p$ -extension of  $F_n$  which is unramified outside the primes of  $F_n$  lying above  $p$ . In fact,  $M_n$  is the field called  $N_n$  in Lemma 1.3, i.e.  $M_n$  is the maximal abelian extension of  $F_n$  contained in  $M_\infty$ . This follows very easily from Lemma 1.5.

Theorem 1.6.  $X_\infty = G(M_\infty/F_\infty)$  is a finitely generated  $\Lambda$ -module.

Proof. Corollary 1.2 shows that  $G(M_\infty/F_\infty)$  is a finitely generated  $\mathbb{Z}_p$ -module, and thus  $X_\infty$  is finitely generated over  $\Lambda$  by Corollary 1.4.

If  $A$  and  $B$  are  $\Lambda$ -modules, we say that  $A$  is pseudo-isomorphic to  $B$  if there exists a  $\Lambda$ -homomorphism from  $A$  to  $B$  with finite kernel and cokernel, and we denote this

symbolically by  $A \sim B$ . Of course, this notion is important because the structure theory of finitely generated  $\Lambda$ -modules (see [19]) classifies such  $\Lambda$ -modules only up to pseudo-isomorphism. Finally, if  $A$  is a  $\Lambda$ -module,  $t(A)$  will denote the  $\Lambda$ -torsion submodule of  $A$ .

Corollary 1.7. There exists an integer  $a \geq 0$ , and non-zero elements  $h_1, \dots, h_r$  of  $\Lambda$  such that  $X_\infty \sim \Lambda^a \oplus t(X_\infty)$ , and

$$t(X_\infty) \sim \bigoplus_{j=1}^r \Lambda/(h_j).$$

For the structure theory (see [19]) shows that the corollary is true for any finitely generated  $\Lambda$ -module.

At present, deeper results about  $X_\infty$  are known only when  $F_\infty/F$  is the cyclotomic  $\mathbb{Z}_p$ -extension. From now on we assume that this is the case.

Theorem 1.8. Assume that  $F_\infty/F$  is the cyclotomic  $\mathbb{Z}_p$ -extension. Then  $X_\infty \sim \Lambda^{r_2} \oplus t(X_\infty)$ .

Proof. The theorem is due to Iwasawa [13]. We sketch a shorter proof due to Greenberg [7], which is more in the spirit of the present lectures, but which gives less

additional information about  $M_\infty$ . We use the notation of §1.1, except we attach a subscript  $n$  to indicate that the objects are associated with  $F_n$ . By Corollary 1.2 and Lemma 1.3, the  $\mathbb{Z}_p$ -rank of  $X_\infty/\omega_n X_\infty$  is equal to  $r_2 p^n + \delta_n$ , where

$$\delta_n = \mathbb{Z}\text{-rank of } E_n - \mathbb{Z}_p\text{-rank of } \overline{\phi_n(E_{n,1})}.$$

One sees easily from the structure theory that the theorem is true if and only if  $\delta_n$  is bounded as  $n \rightarrow \infty$ . To prove the latter assertion, let  $p^t$  be the order of the torsion subgroup of  $\overline{\phi_n(E_{n,1})}$ . Now take  $m$  to be any integer  $\geq t$ . Then we can find units  $e_1, \dots, e_{\delta_n}$ , which form part of a basis of  $E_{n,1}^{p^t}$ , but which are  $p^m$ -th powers in  $U_{n,p}$  for each  $p \in S_n$ . Let  $F_\infty$  be the field obtained by adjoining all  $p$ -power roots of unity to  $F$ . Plainly the field obtained by adjoining to  $F_\infty$  the  $p^m$ -th roots of  $e_1, \dots, e_{\delta_n}$  is an unramified extension of  $F_\infty$  with Galois group isomorphic to the product of  $\delta_n$  copies of  $\mathbb{Z}/p^{m-t}\mathbb{Z}$ . Since  $m$  can be chosen as large as we wish, it can be shown without too much difficulty that the unboundedness of  $\delta_n$  would contradict the fact that the Galois group over  $F_\infty$  of the maximal unramified abelian  $p$ -extension of  $F_\infty$  is a finitely generated  $\Lambda$ -torsion  $\Lambda$ -module (see [13] for the proof of this last result).

1.3. Kummer theory

The role of Kummer theory in these lectures is that it enables us to interpret the part of the Galois group  $X_\infty$  in which we are interested as the Pontrjagin dual of part of the  $p$ -primary subgroup of the ideal class group of  $F_\infty$  (see Theorem 1.12).

For each integer  $m \geq 1$ , we write  $\mu_m$  for the group of  $m$ -th roots of unity. Also, as before, let  $W$  be the group of all  $p$ -power roots of unity. Let  $F_\infty = F(W)$ , and let  $F$  denote the field  $F(\mu_p)$  or  $F(\mu_4)$ , according as  $p$  is odd or even. Put

$$G_\infty = G(F_\infty/F), \quad \Delta = G(F/F), \quad \Gamma = G(F_\infty/F),$$

so that  $G_\infty$  is canonically isomorphic to  $\Delta \times \Gamma$ . Let

$\chi : G_\infty \rightarrow \mathbb{Z}_p^\times$  be the character giving the action of  $G_\infty$  on  $W$ , i.e.,  $\sigma(\zeta) = \zeta^{\chi(\sigma)}$  for all  $\zeta \in W$  and  $\sigma \in G_\infty$ . We write  $\theta, \kappa$  for the restriction (by a slight abuse of language) of  $\chi$  to  $\Delta, \Gamma$ , respectively.

Let  $M_\infty$  denote the maximal abelian  $p$ -extension of  $F_\infty$ , which is unramified outside the primes of  $F_\infty$  above  $p$ , and put

$$X_\infty = G(M_\infty/F_\infty) \quad .$$

Since  $M_\infty$  is plainly Galois over  $F$ ,  $G_\infty$  acts on  $X_\infty$  via inner

automorphisms. This is the representation of  $G_\infty$  which we shall be studying in the rest of these lectures. Since  $F_\infty$  is the cyclotomic  $\mathbb{Z}_p$ -extension of  $F$ , Theorem 1.8 shows that  $X_\infty$  is pseudo-isomorphic to  $\Lambda^{r_2(F)} \oplus t(X_\infty)$ , where  $r_2(F)$  is the number of complex primes of  $F$ , and  $t(X_\infty)$  is the  $\Lambda$ -torsion submodule of  $X_\infty$ .

It is often convenient to decompose  $t(X_\infty)$  into eigenspaces for the action of  $\Delta$ . To do this, we assume that  $p$  is odd, so that the order of  $\Delta$  is prime to  $p$ . Let  $\theta$  be the character of  $\Delta$  defined above (i.e. the character giving the action of  $\Delta$  on  $\mu_p$ ), and let  $e_i$  be the orthogonal idempotent of  $\theta^i$  in  $\mathbb{Z}_p[\Delta]$ . Since  $e_i t(X_\infty)$  is also a finitely generated  $\Lambda$ -module, the structure theory tells us that

$$(1.1) \quad e_i t(X_\infty) \sim \bigoplus_{j=1}^{r_i} \Lambda / (f_{ji}) \quad ,$$

where  $r_i$  is an integer  $\geq 1$ , and the  $f_{ji}$  ( $1 \leq j \leq r_i$ ) are non-zero elements of  $\Lambda$ . We put

$$f_i = \prod_{j=1}^{r_i} f_{ji} \quad ,$$

and call  $f_i$  a characteristic power series for  $e_i t(X_\infty)$ . We stress that (1.1) only determines the ideal  $(f_i)$  in  $\Lambda$  uniquely. Thus  $f_i$  itself is only determined up to a unit in

Λ. Of course, the Weierstrass preparation theorem does provide a canonical choice of  $f_i$ , namely, it shows that there is a unique  $f_i$  which is a power of  $p$  times a distinguished polynomial. But, as we shall see in §4 and §5, this does not seem to be the most natural choice.

Let  $I'_\infty$  be the free abelian group on the non-archimedean primes of  $F_\infty$  which do not lie above  $p$ . Define  $V_\infty$  by the exactness of the sequence

$$0 \rightarrow V_\infty \rightarrow (\mathbb{Q}_p/\mathbb{Z}_p) \otimes F_\infty^\times \xrightarrow{\psi} (\mathbb{Q}_p/\mathbb{Z}_p) \otimes I'_\infty ;$$

here the map  $\psi$  is defined by  $\psi(\alpha \otimes a) = \alpha \otimes (a)'$ , where  $(a)' = \sum_{P \nmid p} v_P(a)P$  (this makes sense because there are only finitely many primes of  $F_\infty$  above each rational prime). The result from Kummer theory which we need is the following. For the proof see [13], §7.

Theorem 1.9. There exists a canonical dual pairing

$$\langle , \rangle : X_\infty \times V_\infty \rightarrow W$$

satisfying  $\langle \sigma x, \sigma u \rangle = \sigma \langle x, u \rangle$  for all  $\sigma \in G_\infty$ .

Here we take  $X_\infty$  with its natural topology as a profinite group, and  $V_\infty$  with the discrete topology. The pairing on



Theorem 1.9 is then a dual pairing in the sense of Pontrjagin. If  $A, B$  are  $G_\infty$ -modules, we always adopt the convention of endowing the group  $\text{Hom}(A, B)$  of homomorphisms from  $A$  to  $B$  with the  $G_\infty$ -structure given by  $(\sigma f)(a) = \sigma f(\sigma^{-1}a)$  for all  $\sigma \in G_\infty$ . Then Theorem 1.9 immediately gives a canonical isomorphism

$$(1.2) \quad \chi_\infty \xrightarrow{\sim} \text{Hom}(V_\infty, W)$$

of  $G_\infty$ -modules. We also assume that  $G_\infty$  acts on tensor products of  $G_\infty$ -modules via the diagonal action, and, of course, that it acts trivially on  $\mathbb{Z}_p$  and  $\mathbb{Q}_p/\mathbb{Z}_p$ . Define the  $G_\infty$ -modules

$$T = \varprojlim_n \mu_{p^n}, \quad T^{(-1)} = \text{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p).$$

Of course, as  $\mathbb{Z}_p$ -modules, both  $T$  and  $T^{(-1)}$  are free of rank 1. If  $D$  is any  $\mathbb{Z}_p$ -module which is also a  $G_\infty$ -module, we define  $D(-1) = D \otimes_{\mathbb{Z}_p} T^{(-1)}$  (with the diagonal action of  $G_\infty$ ). In terms of this twisting by roots of unity, (1.2) is equivalent to the existence of an isomorphism

$$(1.3) \quad \chi_\infty(-1) \xrightarrow{\sim} \text{Hom}(V_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$$

of  $G_\infty$ -modules.

Let  $A_\infty$  be the  $p$ -primary subgroup of the ideal class



group of  $F_\infty$  (thus  $A_\infty = \varinjlim A_n$ , where  $A_n$  is the  $p$ -primary subgroup of the ideal class group of  $F_n$ ). Let  $E_\infty$  be the group of units of the ring of integers of  $F_\infty$ . We omit the proof of the following elementary lemma (see [13], Lemma 10, for the proof of a similar result).

Lemma 1.10. There is an exact sequence of  $G_\infty$ -modules

$$0 \rightarrow (\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}} E_\infty \rightarrow V_\infty \rightarrow A_\infty \rightarrow 0.$$

Corollary 1.11. Assume that  $F$  is totally real, and that  $p \neq 2$ . Then, for each odd integer  $i$ ,  $e_i V_\infty$  is isomorphic to  $e_i A_\infty$  as  $G_\infty$ -modules.

To deduce the corollary from the lemma, we note that each  $F_n$  is totally imaginary quadratic extension of a totally real field. For such a field, the subgroup of its units, which is generated by the roots of unity and the units of the totally real subfield, is of index 1 or 2. Since  $p$  is odd, this implies that  $e_i ((\mathbb{Q}_p/\mathbb{Z}_p) \otimes E_\infty) = 0$  for all odd integers  $i$ .

Theorem 1.12. Assume that  $F$  is totally real, and that  $p$  is

odd. Put  $Y_i = e_i t(X_\infty)$ . Then, for each even integer  $i$ , we have an isomorphism

$$Y_i(-1) \xrightarrow{\sim} \text{Hom}(e_{1-i} A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$$

of  $G_\infty$ -modules.

Proof. It follows from (1.3) and Corollary 1.11 that the  $G_\infty$ -module on the right is isomorphic to  $(e_i X_\infty)(-1)$ , when  $i$  is even. Thus, to complete the proof, we must show that  $e_i X_\infty = e_i t(X_\infty)$  for even integers  $i$ . This follows from Theorem 1.8 since one sees easily that

$$\sum_{\substack{i=1 \\ i \text{ even}}}^{\delta} e_i X_\infty \quad (\delta = [F : F])$$

is isomorphic canonically to the Galois group of the maximal abelian  $p$ -extension of  $F_\infty^+$ , which is unramified outside the primes above  $p$ , over  $F_\infty^+$ ; here  $F_\infty^+$  denotes the maximal totally real subfield of  $F_\infty$ . Alternatively, one can appeal to the fact that  $\text{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$  is  $\Lambda$ -torsion, which is not too difficult to prove by other means.

Recall that  $\gamma_0$  is the fixed topological generator of  $\Gamma$  which we use to define our  $\Lambda$ -module structure from the

$\Gamma$ -module structure. As above, let  $\kappa$  be the character giving the action of  $\Gamma$  on the group of  $p$ -power roots of unity. Put

$$u = \kappa(\gamma_0) \quad .$$

It is easy to see that, if we change the  $\Gamma$ -module structure on the left hand side of (1.1) by tensoring with  $T^{(-1)}$ , then the corresponding change we must make on the right hand side is to replace the variable  $T$  by  $u(1 + T) - 1$ . Thus, if  $i$  is odd and we put  $k = 1 - i$ , Theorem 1.12 implies that there is a pseudo-isomorphism

$$\text{Hom}(e_i A_\infty, \mathbb{Q}_p / \mathbb{Z}_p) \sim \bigoplus_{j=1}^{r_k} \Lambda / (f_{jk}(u(1 + T) - 1)) \quad ,$$

where the  $f_{jk}$  are given by (1.1). In particular, a characteristic power series of the  $\Lambda$ -module  $\text{Hom}(e_i A_\infty, \mathbb{Q}_p / \mathbb{Z}_p)$  ( $i$  odd) is given by

$$g_i(T) = f_{1-i}(u(1 + T) - 1) \quad .$$

For reasons that will become clear in §4, we define the power series  $G_i(T)$  ( $i$  odd) by

$$(1.4) \quad G_i(T) = g_i((1 + T)^{-1} - 1) = f_{1-i}(u(1 + T)^{-1} - 1).$$

Needless to say,  $G_i(T)$  is defined only up to multiplication by a unit in  $\Lambda$ .

#### 1.4. p-adic residue formula

The result in this section, which seems to be new, provides the first evidence that the power series  $G_1(T)$  defined above may be related to p-adic L-functions.

We again assume that  $F$  is totally real. Let  $\zeta(F,s)$  be the complex zeta function of  $F$ , and put

$$(1.5) \quad \zeta_S(F,s) = \zeta(F,s) \prod_{p \in S} (1 - (Np)^{-s}) .$$

It is classical that  $\zeta_S(F,s)$  has a simple pole at  $s = 1$  with residue

$$(1.6) \quad \frac{2^{d-1} h R_\infty}{\sqrt{\Delta}} \prod_{p \in S} (1 - (Np)^{-1}) ,$$

where  $d$  is the degree of  $F$  over  $\mathbb{Q}$ ,  $h$  is the class number,  $R_\infty$  the regulator, and  $\Delta$  (for this section) the discriminant of  $F$  over  $\mathbb{Q}$ . Let  $\zeta_p(F,s)$  be the p-adic zeta function of  $F$ , i.e.  $\zeta_p(F,s)$  is the p-adic analogue of the function (1.5). One suspects that  $\zeta_p(F,s)$  has a simple pole at the point  $s = 1$  in  $\mathbb{Z}_p$ , and that the residue at this pole is the p-adic analogue of (1.6), namely the quantity  $\rho_p(F)$  defined in Theorem 1.13, where  $R_p$  is Leopoldt's p-adic regulator of  $F$ . However, at present this is only known for  $F$  abelian over  $\mathbb{Q}$  (a result due to Leopoldt [16]). Nevertheless, the following parallel result is true for all totally real number

fields  $F$ . We again assume that  $p \neq 2$ .

Theorem 1.13.  $G_1(u^s - 1)/(u^s - u)$  has a pole at  $s = 1$  if and only if the  $p$ -adic regulator  $R_p$  of  $F$  does not vanish. If  $R_p \neq 0$ , this pole is simple, and its residue has the same  $p$ -adic valuation as

$$\rho_p(F) = \frac{2^{d-1} h R_p}{\sqrt{\Delta}} \prod_{p \in S} (1 - (Np)^{-1}) .$$

Since this theorem is new, its complete proof is given in Appendix 1. The reader should also note the equivalent form of Theorem 1.13 given by Lemma 8 of Appendix 1. This is quite useful in practice for computing the order of  $G(M/F_\infty)$ , where  $M$  is the maximal abelian  $p$ -extension of  $F$  unramified outside  $S$ , and  $F_\infty$  the cyclotomic  $\mathbb{Z}_p$ -extension of  $F$ .

Example. Take  $F = \mathbb{Q}(\sqrt{85})$ , and  $p = 3$ . For this field,  $h = 2$ , the fundamental unit is  $\epsilon = (9 + \sqrt{85})/2$ , and 3 splits. Since  $\epsilon^2$  is congruent to 1 modulo 9 but not modulo 27, the power of 3 dividing  $R_3$  is 9. Thus, in this example,  $\rho_p(F)$  is a 3-adic unit. Moreover, Lemma 8 of Appendix 1 shows that the degree of  $M$  over  $F_\infty$  is 3.

## §2. Stickelberger ideals

Let  $F$  be a totally real number field,  $M/F$  a finite abelian extension, and  $G = G(M/F)$ . In this section, we use values of the partial zeta functions to define, for each integer  $n \geq 0$ , an ideal  $I_n(M/F)$  in the integral group ring  $\mathbb{Z}[G]$ . Actually, our definition will depend on a certain integrality hypothesis (labelled  $H_n$  below). So far a complete proof of this hypothesis has only been given for  $F = \mathbb{Q}$  or  $F$  real quadratic (see [5]), but it is almost certain that current work of Deligne and Ribet [6] will establish it for all  $F$ . These ideals  $I_n(M/F)$  seem to play a key role in the study of the Iwasawa module introduced in §1 for two reasons. Firstly, when  $F = \mathbb{Q}$  and  $n = 0$ , a classical theorem of Stickelberger (see §3) asserts that  $I_0(M/\mathbb{Q})$  annihilates the ideal class group of  $M$ . One suspects that the same is true for all totally real base fields  $F$ , but the proof in any case other than  $F = \mathbb{Q}$  seems to be a long way off. Secondly, granted a certain congruence on the values of the partial zeta functions, the  $I_n(M/F)$  can be used to construct the abelian  $p$ -adic  $L$ -functions for  $F$  (see §4). This important connexion between the Stickelberger ideals and the  $p$ -adic  $L$ -functions is due to Iwasawa [12] (in the case  $F = \mathbb{Q}$ ).



### 2.1. The partial zeta functions

Let  $\mathfrak{f}$  be an integral ideal of  $F$ , and  $I(\mathfrak{f})$  the group of fractional ideals of  $F$  which are prime to  $\mathfrak{f}$ . Write  $P_1(\mathfrak{f})$  for the group of principal ideals  $(\alpha)$ , where  $\alpha$  is totally positive and  $v_p(\alpha - 1) \geq v_p(\mathfrak{f})$  for all primes  $p$  which divide  $\mathfrak{f}$ . The quotient group  $I(\mathfrak{f})/P_1(\mathfrak{f})$  is, by definition, the ray class group modulo  $\mathfrak{f}$ . To each ray class (= an element of this quotient group)  $C$ , we can associate a function  $\zeta_{\mathfrak{f}}(C, s)$  of the complex variable  $s$  by defining

$$\zeta_{\mathfrak{f}}(C, s) = \sum (Na)^{-s} \quad (R(s) > 1) \quad ,$$

where  $a$  runs over all integral ideals in  $C$ , and  $Na$  denotes the absolute norm of  $a$ . The analytic continuation of the complex L-functions implies that each  $\zeta_{\mathfrak{f}}(C, s)$  can be analytically continued over the whole complex plane, except for a simple pole at  $s = 1$ . If  $b$  is a representative of  $C$ , we often write  $\zeta_{\mathfrak{f}}(b, s)$  instead of  $\zeta_{\mathfrak{f}}(C, s)$ . We call  $\zeta_{\mathfrak{f}}(C, s)$  the partial zeta function of  $C$ .

Suppose now that  $M$  is a finite abelian extension of  $F$ , and let  $\mathfrak{f}$  be its conductor. If  $a$  is a fractional ideal of  $F$  which is prime to  $\mathfrak{f}$ , write  $(a, M/F)$  for the Artin symbol of  $a$ . For each  $\sigma$  in the Galois group of  $M$  over  $F$ , we define



$$\zeta_M(\sigma, s) = \sum (Na)^{-s} \quad (R(s) > 1) \quad ;$$

here  $a$  runs over all integral ideals of  $F$  prime to  $\mathfrak{f}$  such that  $\sigma = (a, M/F)$ . Plainly

$$\zeta_M(\sigma, s) = \sum_{\mathfrak{C}} \zeta_{\mathfrak{C}}(\sigma, s) \quad ,$$

where the sum on the right is taken over all ray classes modulo  $\mathfrak{C}$  such that  $(\mathfrak{C}, M/F) = \sigma$ . More generally, the following lemma is plain from the behaviour of the Artin map under restriction.

Lemma 2.1. Let  $L, M$  be finite abelian extensions of  $F$ , with  $M$  contained in  $L$ . Assume that each non-archimedean prime of  $F$  which is ramified in  $L$  is also ramified in  $M$ . Then, for each  $\sigma \in G(M/F)$ , we have

$$\sum_{\tau|_{M=\sigma}} \zeta_L(\tau, s) = \zeta_M(\sigma, s) \quad ,$$

where  $\tau$  runs over all elements of  $G(L/F)$  whose restriction to  $M$  is  $\sigma$ .

After earlier work of Klingen, Siegel [22] proved the following basic fact using modular forms.

Theorem 2.2. For each  $\sigma \in G(M/F)$ , and each integer  $n \geq 0$ ,

$\zeta_M(\sigma, -n)$  is rational.

Explicit formulae for these rational numbers  $\zeta_M(\sigma, -n)$  are known only when  $F = \mathbb{Q}$  (Hurwitz [9]) and  $F$  real quadratic (Siegel [21]).

## 2.2. The norm congruence lemma

Let  $L$  be a number field, and  $n$  a positive integer.

We define  $w_n(L)$  to be the largest integer  $m$  such that  $G(L(\mu_m)/L)$  has exponent dividing  $n$ . In particular,  $w_1(L)$  is the number of roots of unity in  $L$  itself.

We call a set  $S$  of fractional ideals of  $F$  dense if, for any finite abelian extension  $M/F$ , and any  $\sigma \in G(M/F)$ , we have  $\sigma = (a, M/F)$  for some  $a \in S$ . For example, the set consisting of all integral ideals of  $F$  which are relatively prime to a given finite set of prime ideals is dense. The following lemma was first pointed out to me by Sinnott, although it is probably well known to others.

Lemma 2.3. Let  $p$  be a rational prime, and let  $S$  be a dense set of fractional ideals, all of whose elements are prime to  $p$ . If  $M$  is a finite abelian extension of  $F$ , and  $n$  is a

positive integer, then

$$\left| w_n(M) \right|_p^{-1} = \min_{\substack{a \in S \\ (a, M/F)=1}} |Na^n - 1|_p^{-1},$$

where the minimum is taken over all ideals  $a$  in  $S$  such that  $(a, M/F)$  is defined and equal to the identity.

Proof. This is just an exercise in the formal properties of the Artin symbol. Let  $S_1$  denote the subset of  $S$  containing all  $a$  such that  $(a, M/F)$  is defined and equal to 1. The lemma follows immediately from the equivalence of the following five statements:- (i)  $p^e$  divides  $w_n(M)$  (e some integer  $\geq 0$ ), (ii)  $\sigma^n = 1$  for all  $\sigma \in G(M(\mu_p^e)/M)$ , (iii)  $(a, M(\mu_p^e)/F) = 1$  for all  $a \in S_1$ , (iv)  $\zeta^{Na^n} = \zeta$  for all  $\zeta \in \mu_p^e$  and all  $a \in S_1$ , and (v)  $p^e$  divides  $Na^n - 1$  in  $\mathbb{Z}_p$  for all  $a \in S_1$ .

### 2.3. Integrality

Let  $b, c, \mathfrak{f}$  be integral ideals of  $F$  with  $bc$  prime to  $\mathfrak{f}$ . For each integer  $n \geq 0$ , we define

$$(2.1) \quad \delta_n(b, c; \mathfrak{f}) = (Nc)^{n+1} \zeta_{\mathfrak{f}}(b, -n) - \zeta_{\mathfrak{f}}(bc, -n)$$

Consider the following integrality hypothesis for  $F$  and  $n$ .

Hypothesis  $H_n$ . If  $p$  is a rational prime which does not divide  $Nc$ , then  $\delta_n(b, c; \mathfrak{f})$  is integral at  $p$ .

For each integer  $n \geq 0$ ,  $H_n$  is true for  $F = \mathbb{Q}$  and  $F$  real quadratic (see [5]). As mentioned before, the work of Deligne and Ribet [6] will almost certainly establish  $H_n$  for all totally real  $F$  and all  $n \geq 0$ .

Now let  $M$  be any finite abelian extension of  $F$ . For each  $\sigma \in G(M/F)$ , and each integral ideal  $c$  of  $F$  which is prime to the conductor of  $M/F$ , we define

$$(2.2) \quad \delta_n(\sigma, c; M) = (Nc)^{n+1} \zeta_M(\sigma, -n) - \zeta_M(\sigma(c, M/F), -n) .$$

The next theorem was pointed out to me by Sinnott.

Theorem 2.4. Assume that hypothesis  $H_n$  is true for  $F$ . Then, for each finite abelian extension  $M$  of  $F$  and each  $\sigma \in G(M/F)$ , we have (i)  $w_{n+1}(M) \zeta_M(\sigma, -n)$  is an integer, and (ii)  $\delta_n(\sigma, c; M)$  is an integer for each integral ideal  $c$  of  $F$  which is prime to  $w_{n+1}(M)$  and the conductor of  $M/F$ .

Proof. Let  $\mathfrak{f}$  be the conductor of  $M/F$ , and let  $L$  be the ray

class field with conductor  $\mathfrak{f}$ . Then  $\zeta_L((b, L/F), s) = \zeta_{\mathfrak{f}}(b, s)$ , so that Lemma 2.1 gives

$$\sum_{\substack{b \bmod \mathfrak{f} \\ (b, M/F) = \sigma}} \delta_n(b, c; \mathfrak{f}) = \delta_n(\sigma, c; M) \quad ;$$

here  $b$  runs over a set of representatives of the ray classes modulo  $\mathfrak{f}$  such that  $(b, M/F) = \sigma$ . By hypothesis  $H_n$ , the left hand side is  $p$ -integral if  $p$  does not divide  $Nc$ , and so the same is true on the right. Fix a prime number  $p$ . Letting  $c$  range over all integral ideals prime to  $\mathfrak{f}$  and  $p$  such that  $(c, M/F) = 1$ , we conclude from Lemma 2.3 that

$w_{n+1}(M) \zeta_M(\sigma, -n)$  is  $p$ -integral. Since  $p$  was arbitrary, this proves (i). Now suppose that  $c$  is integral and prime to  $\mathfrak{f}$  and  $w_{n+1}(M)$ . Again let  $p$  be any prime. If  $p$  does divide  $w_{n+1}(M)$ , then  $\delta_n(\sigma, c; M)$  is integral at  $p$  because  $p$  does not divide  $Nc$ . On the other hand, if  $p$  does not divide  $w_{n+1}(M)$ , then  $\delta_n(\sigma, c; M)$  is  $p$ -integral by (i). Thus (ii) is proven.

#### 2.4. The Stickelberger ideals.

Let  $M$  be a finite abelian extension of  $F$ , and  $G = G(M/F)$ . For each integer  $n \geq 0$ , define the  $n$ -th Stickelberger element  $\alpha_n(M) \in \mathbb{Q}[G]$  for  $M/F$  by

$$\alpha_n(M) = \sum_{\sigma \in G} \zeta_M(\sigma, -n) \sigma^{-1}.$$

The study of these elements when  $n = 0$  as generalizations of the classical Stickelberger element for abelian extensions of  $\mathbb{Q}$  was first suggested by Brumer (see [18]). If  $c$  is an integral ideal prime to the conductor of  $M/F$ , we plainly have

$$((Nc)^{n+1} - (c, M/F)) \alpha_n(M) = \sum_{\sigma \in G} \delta_n(\sigma, c; M) \sigma^{-1},$$

where the  $\delta_n(\sigma, c; M)$  are defined by (2.2). Suppose now that hypothesis  $H_n$  is valid for  $F$ . Then Theorem 2.4 shows that the right hand side of the above equation lies in the integral group ring  $\mathbb{Z}[G]$ , provided  $c$  is prime to  $w_{n+1}(M)$ . We therefore define  $I_n(M/F)$ , the  $n$ -th Stickelberger ideal of  $M/F$ , to be the ideal of  $\mathbb{Z}[G]$  generated by the elements

$$(2.3) \quad (Nc^{n+1} - (c, M/F)) \alpha_n(M)$$

for  $c$  ranging over all integral ideals of  $F$  which are prime to  $w_{n+1}(M)$  and the conductor of  $M/F$ .

**Lemma 2.5.** Assume that hypothesis  $H_n$  is valid for  $F$ . Then

(i)  $w_{n+1}(M) \alpha_n(M)$  belongs to  $I_n(M/F)$ , and (ii)  $I_n(M/F)$  is in fact generated by the elements (2.3) for  $c$  ranging over

all integral ideals of  $F$  which are relatively prime to  $w_{n+1}(M)$ , the conductor of  $M/F$ , and any given finite set of primes.

Indeed, Lemma 2.3 implies that  $w_{n+1}(M)$  is the greatest common divisor of the set  $\{Nc^{n+1} - 1\}$ , where  $c$  ranges over all integral ideals of  $F$ , relatively prime to the conductor of  $M/F$  and  $w_{n+1}(M)$ , which satisfy  $(c, M/F) = 1$ . This establishes (i). For the proof of (ii), which is not obvious, see [5].

### §3. Stickelberger's theorem

The aim of this section is to prove Stickelberger's theorem. We use the notation of §2.

Theorem 3.1. Let  $M$  be a finite abelian extension of  $\mathbb{Q}$ . Then  $I_0(M/\mathbb{Q})$  annihilates the ideal class group of  $M$ .

The theorem is nontrivial only when  $M$  is imaginary, since one sees easily that  $\alpha_0(M) = 0$  when  $M$  is real. Our proof is the same as Stickelberger's [23], and is based on the factorization of Gauss sums. It would be interesting to



find an alternative proof.

Corollary 3.2. Let  $M$  be an imaginary quadratic field, and  $L(\psi, s)$  the Dirichlet  $L$ -function of  $M$ . Then  $2w_1(M)L(\psi, 0)$  annihilates the ideal class group of  $M$ .

Of course, in this case, the analytic class number formula tells us that the order of the ideal class group of  $M$  is actually equal to the absolute value of  $w_1(M)L(\psi, 0)$ . We have mentioned the corollary because its proof is not analytic, and is essentially different from that of the analytic class number formula. It is also of interest to note that historically the proof of the corollary preceded the proof of the analytic class number formula.

We mention an analogue of Theorem 3.1, although we do not prove it in these lectures. To motivate this analogue, we recall that we can view the ideal class group of  $M$  as the (reduced) Grothendieck group  $K_0^0$ , where  $\mathcal{O}$  is the ring of integers of  $M$ . Let  $K_2^0$  be as defined by Milnor [17]. It has a natural structure as a  $\mathbb{Z}[G]$ -module. It is also known that  $K_2^0$  is finite.

Theorem 3.3. Let  $M$  be a finite abelian extension of  $\mathbb{Q}$ . Then  $I_1(M/\mathbb{Q})$  annihilates  $K_2^0$ , except perhaps for the 2-primary subgroup.

Just as above for the classical Stickelberger theorem, one sees almost immediately that Theorem 3.3 has the following corollary. Let  $\zeta(M,s)$  be the complex zeta function of  $M$ .

Corollary 3.4 Let  $M$  be a real quadratic field. Then  $w_2(M)\zeta(M,-1)$  annihilates  $K_2^0$ , except perhaps for the 2-primary subgroup.

The Birch-Tate conjecture predicts that the order of  $K_2^0$  is equal to the absolute value of  $w_2(M)\zeta(M,-1)$ . But, in contrast to the class number formula, this has only been proven in a few cases. For the proof of Theorem 3.3, see [4], [5]. Finally, we remark that the obvious guess is that, for each integer  $n \geq 0$ ,  $I_n(M/\mathbb{Q})$  annihilates  $K_{2n}^0$ , where these are the higher K-groups defined by Quillen.

### 3.1. Gauss sums

Let  $p$  be a prime number, and  $\mathbb{C}_p$  the algebraic

closure of  $\mathbb{Q}_p$ . Throughout §3.1, we assume that all characters take their values in  $\mathbb{C}_p$ . For each integer  $m \geq 1$ , we write, as usual,  $\mu_m$  for the group of  $m$ -th roots of unity in  $\mathbb{C}_p$ .

Let  $q = p^n$ , and let  $F_q$  be the finite field with  $q$  elements. The Gauss sums we will be interested in are those of the form

$$G(\chi, \psi) = \sum_{a \in F_q^\times} \chi(a) \psi(a),$$

where  $\psi$  is a character of the additive, and  $\chi$  a character of the multiplicative group of  $F_q$ . If  $m$  is the order of  $\chi$ , it is plain that  $G(\chi, \psi)$  belongs to  $\mathbb{Q}(\mu_{mp})$ . We omit the proof of the following elementary lemma.

Lemma 3.5. (i) If  $m$  is the order of  $\chi$ , then  $G(\chi, \psi)^m \in \mathbb{Q}(\mu_m)$ ; (ii) If both  $\chi$  and  $\psi$  are non-trivial, then  $G(\chi, \psi)$  has absolute value  $\sqrt{q}$  at each archimedean valuation of  $\mathbb{Q}(\mu_{mp})$ .

Let  $K$  denote the unramified extension of  $\mathbb{Q}_p$  with residue field  $F_q$ . Then  $\mu_{q-1} \subset K$  is mapped isomorphically under reduction modulo  $p$  to  $F_q^\times$ . Let  $\text{Tr}$  denote the trace

from  $K$  to  $\mathbb{Q}_p$ . One sees easily that any  $G(\chi, \psi)$  can be written in the form

$$G_k = \sum_{\alpha \in \mu_{q-1}} \alpha^{-k} \varepsilon^{\text{Tr}(\alpha)} ,$$

for some integer  $k$  and some  $\varepsilon \in \mu_p$ . Note also that each integer  $k$  with  $0 < k < q - 1$  can be written uniquely in the form

$$(3.1) \quad k = \sum_{j=0}^{n-1} k_j p^j , \quad \text{where } 0 \leq k_j < p .$$

Theorem 3.6. Let  $\pi = \varepsilon - 1$ . Then, for  $0 < k < q - 1$ , we have

$$G_k \equiv - \frac{\pi^{k_0 + \dots + k_{n-1}}}{k_0! \dots k_{n-1}!} \pmod{\pi^{k_0 + \dots + k_{n-1} + 1}} ,$$

where  $k_0, \dots, k_{n-1}$  are defined by (3.1).

Proof. Note that  $\pi$  is a local parameter in  $K(\varepsilon)$ . If  $z$  is in  $\mathbb{Z}_p$ , we have

$$\varepsilon^z = (1 + \pi)^z = \sum_{i=0}^{\infty} \binom{z}{i} \pi^i .$$

Taking  $z = \text{Tr}(\alpha)$ , we obtain

$$G_k = \sum_{i=0}^{\infty} A_{k,i} \pi^i , \quad \text{where } A_{k,i} = \sum_{\alpha \in \mu_{q-1}} \alpha^{-k} \binom{\text{Tr}(\alpha)}{i} .$$

Our aim is to find the smallest integer  $i \geq 0$  such that

$A_{k,i} \neq 0$ . We begin with an observation. Let  $k_0, \dots, k_{n-1}$  be defined by (3.1). Then we claim that

$$(3.2) \quad \sum_{j=0}^{n-1} k_j = \min \left\{ \sum_{j=0}^{n-1} h_j : \sum_{j=0}^{n-1} h_j p^j \equiv k \pmod{(q-1)}, h_j \geq 0 \right\},$$

with the minimum being obtained only when

$h_0 = k_0, \dots, h_{n-1} = k_{n-1}$ . Indeed, if one of the  $h_j$ , say  $h_\lambda$ ,

is greater than or equal to  $p$ , one can decrease  $\sum_{j=0}^{n-1} h_j$

by replacing  $h_\lambda$  by  $h_\lambda - p$  and  $h_{\lambda+1}$  (resp.  $h_0$  if  $\lambda = n-1$ )

by  $h_{\lambda+1} + 1$  (resp.  $h_0 + 1$ ). But if all the  $h_j$  are  $< p$ ,

we plainly must have  $h_j = k_j$  for  $0 \leq j < n$ .

Next we note that the formal identity

$$(1 + T)^{x_0} + \dots + (1 + T)^{x_{n-1}} = \sum_{j=0}^{n-1} (1 + T)^{x_j}$$

gives

$$\binom{x_0 + \dots + x_{n-1}}{i} = \sum \binom{x_0}{i_0} \dots \binom{x_{n-1}}{i_{n-1}},$$

where the sum on the right is over all non-negative integers

$i_0, \dots, i_{n-1}$  with sum  $i$ . Recalling that  $\text{Tr}(\alpha) = \sum_{j=0}^{n-1} \alpha^{p^j}$  for

$\alpha \in \mu_{q-1}$  we obtain

$$A_{k,i} = \sum_{\alpha \in \mu_{q-1}} \alpha^{-k} \left( \sum \binom{\alpha^p}{i_0} \dots \binom{\alpha^p}{i_{n-1}} \right),$$

where the sum in brackets on the right is again over all non-negative integers  $i_0, \dots, i_{n-1}$  with sum  $i$ . Now it is plain that

$$\begin{aligned} & \binom{\alpha^p}{i_0} \dots \binom{\alpha^p}{i_{n-1}} \\ &= \sum c(e_0, \dots, e_{n-1}) \alpha^{e_0 p^0 + \dots + e_{n-1} p^{n-1}}, \end{aligned}$$

where the sum on the right is taken over all integers

$e_0, \dots, e_{n-1}$  with  $0 \leq e_j \leq i_j$  ( $0 \leq j < n$ ), and the

$c(e_0, \dots, e_{n-1})$  are rational numbers. But  $\sum_{\alpha \in \mu_{q-1}} \alpha^h = 0$

unless  $h \equiv 0 \pmod{q-1}$ . Thus, if  $A_{k,i} \neq 0$ , there must

exist integers  $i_0, \dots, i_{n-1}$  with sum  $i$ , and integers

$e_0, \dots, e_{n-1}$  such that

$$0 \leq e_j \leq i_j \quad (0 \leq j < n), \quad \sum_{j=0}^{n-1} e_j p^j \equiv k \pmod{q-1}.$$

It follows immediately from (3.2) that we must have

$i \geq k_0 + \dots + k_{n-1}$ . Also, if  $i = k_0 + \dots + k_{n-1}$ , (3.2)

tells us that

$$A_{k,i} = (q-1)/(k_0! \dots k_{n-1}!) \equiv (-1)/(k_0! \dots k_{n-1}!) \pmod{q}.$$

This completes the proof of Theorem 3.6.

If  $x$  is a real number, we write  $[x]$  for the largest integer  $\leq x$ , and put  $\{x\} = x - [x]$ . If  $h$  is any integer, let  $k = k(h)$  be the least non-negative residue of  $h \bmod q-1$ , and then let the integers  $k_i$  with  $0 \leq k_i < p$  be given by the expansion (3.1) of  $k$ . We define

$$s(h) = k_0 + \dots + k_{n-1}.$$

Lemma 3.7 For each integer  $h$ , we have

$$(p-1) \sum_{i=0}^{n-1} \{p^i h / (q-1)\} = s(h).$$

Proof. Since both sides of the previous equation are unchanged when we add to  $h$  a multiple of  $q-1$ , we can suppose that  $0 \leq h < q-1$ . Hence  $h = \sum_{j=0}^{n-1} k_j p^j$ , where  $0 \leq k_j < p$ . Let  $i$  be any integer satisfying  $0 \leq i \leq n-1$ . Since  $q = p^n$ , we evidently have

$$p^i h \equiv \sum_{j=0}^{n-i-1} k_j p^{i+j} + \sum_{j=n-i}^{n-1} p^{i+j-n} k_j \bmod (q-1).$$

Since the expression on the right is  $< q-1$ , it must be the least non-negative residue of  $p^i h$ , i.e., it must be



$(q-1) \{p^i h / (q-1)\}$ . Summing from  $i = 0$  to  $n - 1$ , we conclude that

$$(q - 1) \sum_{i=0}^{n-1} \{p^i h / (q-1)\} = \left( \sum_{j=0}^{n-1} k_j \right) \left( \sum_{j=0}^{n-1} p^j \right),$$

which is just a slightly modified form of the lemma.

### 3.2. Proof of Stickelberger's theorem

(i). Until further notice, we assume that  $M$  is the full cyclotomic field  $M = \mathbb{Q}(\mu_f)$ , where  $f$  is either odd or divisible by 4. Let  $p$  be a prime ideal of  $M$  which does not divide  $f$ . Let  $\chi_p$  be the  $f$ -th power residue symbol relative to  $p$ , i.e., for  $x$  prime to  $p$ ,  $\chi_p(x)$  is the unique  $f$ -th root of unity congruent to  $x^{\frac{q-1}{f}} \pmod{p}$ , where  $q = Np$ . We view  $\chi_p$  as a character of the multiplicative group of the residue field of  $p$ , and take  $\psi$  to be any non-trivial character of the additive group.

Proposition 3.8.  $G(\chi_p, \psi)^f$  belongs to  $M$ , and the factorization of the ideal  $(G(\chi_p, \psi)^f)$  is  $p^{f\beta(M)}$ , where

$$\beta(M) = \sum_{\substack{c \pmod{f} \\ (c, f)=1}} (1 - \{\frac{c}{f}\}) (c, M/\mathbb{Q})^{-1}.$$

Proof. We identify positive integers with the ideals they generate in  $\mathbb{Z}$ . For the proof, we can suppose that  $M$  is embedded in  $\mathbb{C}_p$  in such a way that the valuation of  $M$  defined by  $p$  coincides with that of  $\mathbb{C}_p$  (we then regard  $M$  as a subset of  $\mathbb{C}_p$ ). For each positive integer  $c$  prime to  $f$ , write  $\sigma_c$  for the Artin symbol  $(c, M/\mathbb{Q})$  of  $c$ . Plainly  $\sigma_c$  maps the valuation of  $M$  defined by  $p^c$  to the valuation of  $\mathbb{C}_p$ . It is also easy to see that  $\sigma_c$  maps  $G(\chi_p, \psi)^f$  to  $G(\chi_p^c, \psi)^f$ . As the ramification index of  $M(\mu_p)$  over  $M$  is  $p-1$ , it follows from Theorem 3.6 that the order of  $G(\chi_p, \psi)^f$  at  $p^{c-1}$  is  $fs(r)/(p-1)$ , where  $r = -c(q-1)/f$ . On the other hand, since  $q = p^n$ , the decomposition group of  $p$  in  $M$  consists of the elements  $(p^i, M/\mathbb{Q})$  ( $0 \leq i \leq n-1$ ). Since  $1 - \{x\} = \{-x\}$  for any  $x$  not in  $\mathbb{Z}$ , it follows that the power of  $p^{c-1}$  occurring in  $p^{f\beta(M)}$  is  $f \sum_{i=0}^{n-1} \{-p^i c/f\} = fs(r)/(p-1)$ . The last equality is valid by virtue of Lemma 3.7.

It is convenient to give a slightly modified version of Proposition 3.8. Let  $p$  be a prime of  $M$  which does not divide  $w_1(M)$ , and, as usual, let  $q = p^n = Np$ . Define

$$\tau(p) = G(\chi_p, \psi) / \sqrt{q^*},$$

where  $q^*$  is either  $p^n$  or  $(-p)^n$ , according as  $p \equiv 1$  or  $3$

mod 4 (the choice of which square root of  $q^*$  we take is not important). Since  $\sqrt{q^*}$  belongs to  $\mathbb{Q}(\mu_p)$ , we have  $\tau(p) \in M(\mu_p)$ . We extend  $\tau$  by multiplicativity to the group of all fractional ideals of  $M$  which are prime to  $w_1(M)$ . Since Hurwitz's explicit formulae for the values of the partial zeta functions of  $\mathbb{Q}$  at the non-positive integers show, in particular, that

$$\zeta_f(c, 0) = -\{c/f\} + 1/2 \quad ,$$

the next result is an immediate consequence of proposition 3.8.

Proposition 3.8\* For each ideal  $a$  prime to  $w_1(M)$ ,  $\tau(a)^{w_1(M)}$  belongs to  $M$ , and

$$a^{w_1(M)} \alpha_o(M) = (\tau(a)^{w_1(M)}) \quad .$$

Thus Proposition 3.8\* shows that the element  $w_1(M) \alpha_o(M)$  of  $I_o(M/\mathbb{Q})$  annihilates the ideal class group of  $M$ . To prove that the same is valid for the whole Stickelberger ideal  $I_o(M/\mathbb{Q})$ , one can either argue explicitly with Jacobi sums (which is the more traditional way), or invoke a Kummer theory argument due to Leopoldt [16]. We follow the latter course. Let  $c$  be a positive integer prime to  $w_1(M)$ , and

put  $\sigma_c = (c, M/\mathbb{Q})$ . For each fractional ideal  $a$  of  $M$  prime to  $w_1(M)$ , we define

$$(3.3) \quad \lambda_c(a) = \tau(a)^c / \tau(a^{\sigma_c}) .$$

A priori,  $\lambda_c(a)$  belongs to some cyclotomic extension of  $M$ .

Proposition 3.9.  $\lambda_c(a)$  belongs to  $M$ , and

$$a^{(c-\sigma_c)\alpha_o(M)} = (\lambda_c(a)) .$$

Proof. We can plainly suppose that  $a$  is a prime ideal  $p$ .

Put  $K = M(\lambda_c(p))$ , so that  $K \subset M(\mu_p)$ . By Proposition 3.8\*, the  $w_1(M)$ -th power of  $\lambda_c(p)$  belongs to  $M$ , and thus  $K/M$  is a Kummer extension. Moreover, Proposition 3.8\* also shows that

$$p^{w_1(M)(c-\sigma_c)\alpha_o(M)} = (\lambda_c(p)^{w_1(M)}) .$$

Since  $(c - \sigma_c)\alpha_o(M)$  belongs to the integral group ring

because  $c$  is prime to  $w_1(M)$ , it follows that the ideal  $(\lambda_c(p)^{w_1(M)})$  is a  $w_1(M)$ -th power. Hence every prime of  $M$

which ramifies in  $K$  must divide  $d = [K:M]$ , and so must

certainly divide  $w_1(M)$ . On the other hand,  $K$  is an inter-

mediate field between  $M$  and  $M(\mu_p)$ . But  $M(\mu_p)/M$  is totally

ramified at the primes above  $p$ , and, as  $(p, w_1(M)) = 1$ , it follows that  $K = M$ . This completes the proof.

Lemma 3.10. For each  $\sigma \in G(M/\mathbb{Q})$ , we have  $\lambda_c(a)^\sigma = \lambda_c(a^\sigma)$ .

Proof. Again we suppose that  $\mathfrak{a}$  is a prime ideal  $\mathfrak{p}$ . Pick  $\tilde{\sigma}$  in the Galois group of  $M(\mu_p)$  over  $\mathbb{Q}(\mu_p)$  such that the restriction of  $\tilde{\sigma}$  to  $M$  is  $\sigma$  (this is possible because  $(p, f) = 1$ ). Since  $\chi_p(x)^\sigma = \chi_{p^\sigma}(x^\sigma)$ , we deduce easily from the explicit expression for our Gauss sums that  $G(\chi_p, \psi)^\sigma = G(\chi_{p^\sigma}, \psi)$ . Hence  $\tau(\mathfrak{p})^\sigma = \tau(\mathfrak{p}^\sigma)$ , and the result follows.

(ii). Now take  $M/\mathbb{Q}$  to be any finite abelian extension, and let  $f$  be its conductor so that  $M \subset \mathbb{Q}(\mu_f)$ . Let  $j$  be the natural inclusion of the ideal group of  $M$  in the ideal group of  $\mathbb{Q}(\mu_f)$ . Let  $c$  be a positive integer prime to  $f$  and  $w_1(M)$ , or equivalently prime to  $2f$ . If  $\mathfrak{a}$  is an ideal of  $M$  prime to  $2f$ , Lemma 3.10 plainly shows that  $\lambda_c(j(\mathfrak{a}))$  belongs to  $M$ , where  $\lambda_c$  is defined by (3.3). Also, by Lemma 2.1, the restriction of  $\alpha_o(\mathbb{Q}(\mu_f))$  to  $M$  is equal to  $\alpha_o(M)$ . Hence Proposition 3.9 implies that

$$\underset{\mathfrak{a}}{(c-(c, M/\mathbb{Q}))\alpha_o(M)} = (\lambda_c(j(\mathfrak{a}))) .$$

This completes the Proof of Theorem 3.1.

#### §4. p-adic L-functions

We now show how the Stickelberger ideals for abelian extensions of a totally real base field  $F$  can be used to construct the abelian p-adic L-functions of  $F$ . This important idea (in the case  $F = \mathbb{Q}$ ) is due to Iwasawa [12]. Actually, it is misleading to say that we carry out the construction in this section. We only do so assuming two hypotheses (labelled  $D(p)$  and  $C(p)$  below) on the values of the partial zeta functions of  $F$ . The real difficulty lies in the proof of these hypotheses. So far they have only been proven for  $F = \mathbb{Q}$  or  $F$  real quadratic (see [3], [5]), but again the work of Deligne and Ribet will almost certainly establish them in general.

##### 4.1. Values of L-functions

Let  $M$  be a finite abelian extension of  $F$ , and  $\chi$  a 1-dimensional character of  $G = G(M/F)$  with values in  $\mathbb{C}_p$  (= the algebraic closure of  $\mathbb{Q}_p$ ). Replacing  $M$  by the fixed field of the kernel of  $\chi$  if necessary, we can suppose that the kernel of  $\chi$  is trivial. For each integer  $n \geq 0$ , we



define

$$L(\chi, -n) = \sum_{\sigma \in G} \chi(\sigma) \zeta_M(\sigma, -n) \quad .$$

Of course, if  $\chi$  was a character of  $G$  with values in  $\mathbb{C}$  rather than  $\mathbb{C}_p$ , this would simply be the value of the complex L-function of  $\chi$  at  $-n$ . Let  $S$  be the set of primes of  $F$  above  $p$ . We also define

$$L_S(\chi, -n) = \sum_C \chi(C) \zeta_g(C, -n) \quad ,$$

where  $g$  is the least common multiple of  $(p)$  and the conductor of  $\chi$ , and  $C$  runs over the ray classes modulo  $g$ . Note that, by Lemma 2.1, we could replace  $g$  in the last definition by any integral ideal which is (i) divisible by the conductor of  $\chi$ , and (ii) divisible by precisely those prime ideals which divide  $p$  and the conductor of  $\chi$ . Also, it is easy to see that

$$L_S(\chi, -n) = L(\chi, -n) \prod_{p \in S} (1 - \chi(p) (Np)^n).$$

#### 4.2. Construction of the $G(T, \chi)$ .

The following general principle lies behind the construction in this section. Let  $\mathcal{O}$  be the ring of integers of a finite extension of  $\mathbb{Q}_p$ , and  $\Lambda$  the ring of formal power series in an indeterminate  $T$  with coefficients in  $\mathcal{O}$ . Let



$F_\infty$  be the cyclotomic  $\mathbb{Z}_p$ -extension of  $F$ . For each  $n \geq 0$ , let  $\Sigma_n = G(F_n/F)$ , and let  $\mathcal{O}[\Sigma_n]$  be the group ring of  $\Sigma_n$  with coefficients in  $\mathcal{O}$ . Fix a topological generator  $\gamma_0$  of  $\Gamma = G(F_\infty/F)$ . We view  $\Lambda$  as being endowed with the topology defined by the powers of its maximal ideal  $\mathfrak{m}$ .

Lemma 4.1. There is a unique topological isomorphism of  $\mathcal{O}$ -algebras

$$\Phi : \varprojlim \mathcal{O}[\Sigma_n] \xrightarrow{\sim} \Lambda$$

satisfying  $\Phi(\gamma_0) = 1 + T$ .

For the proof of this lemma, see [19].

To carry out the construction, we need the following weaker version of hypothesis  $H_0$  of §2. Recall that  $\delta_0(b, c; \mathfrak{f})$  is given by (2.1).

Hypothesis D(p). Let  $b, c, \mathfrak{f}$  be integral ideals of  $F$ , with  $bc$  prime to  $\mathfrak{f}$ , and  $\mathfrak{f}$  divisible by all primes above  $p$ . Then  $\delta_0(b, c; \mathfrak{f})$  is integral at  $p$ .

As mentioned before,  $D(p)$  is true for  $F = \mathbb{Q}$  or  $F$  real quadratic and all primes  $p$ . Again Deligne and Ribet will

almost certainly prove it in general.

Let  $M/F$  be a finite abelian extension with Galois group  $G$ , and  $\chi$  a faithful 1-dimensional character of  $G$  with values in  $\mathbb{C}_p$ . Let  $q$  denote  $p$  or  $4$  according as  $p$  is odd or even, and put

$$M_0 = M(\mu_q) \quad , \quad M_\infty = M(W) \quad .$$

Let the integer  $e \geq 0$  be such that  $q_0 = qp^e$  is the order of the group of all  $p$ -power roots of unity of  $M_0$ . For each  $n \geq 0$ , define  $q_n = q_0 p^n$ . Then it is plain that the  $n$ -th layer of  $M_\infty/M_0$  is given by  $M_n = M(\mu_{q_n})$ . Let  $G_n = G(M_n/F)$ . Recall that the 0-th Stickelberger element for  $M_n/F$  is defined by

$$\xi_n = \alpha_0(M_n) = \sum_{\sigma \in G_n} \zeta_{M_n}(\sigma, 0) \sigma^{-1} \quad .$$

Take  $c \neq 1$  to be any integral ideal of  $F$  prime to both  $p$  and the conductor of  $\chi$ . As before, we have

$$(4.1) \quad (Nc - (c, M_n/F)) \xi_n = \sum_{\sigma \in G_n} \delta_0(\sigma, c; M_n) \sigma^{-1} \quad ,$$

where  $\delta_0(\sigma, c; M_n)$  is given by (2.2). Now it is easy to see that there exists an integer  $n_0 \geq 0$  such that, for all  $n \geq n_0$ , the same primes of  $F$  ramify in  $M_n$ , namely those which divide either  $p$  or the conductor of  $\chi$ . Thus, assuming that  $D(p)$

is valid for  $F$  and  $p$ , we conclude from Lemma 2.1 that

(4.1) lies in the integral group ring  $\mathbb{Z}_p[G_n]$  for all

$n \geq n_0$ .

Plainly  $M_n$  contains the  $(n + e)$ -th layer  $F_{n+e}$  of the cyclotomic  $\mathbb{Z}_p$ -extension of  $F$ . Write  $r_n$  for the restriction map from  $G_n$  to  $\Sigma_{n+e} = G(F_{n+e}/F)$ . Let  $0_\chi$  be the ring of integers of the field obtained by adjoining the values of  $\chi$  to  $\mathbb{Q}_p$ . We define a ring homomorphism from  $0_\chi[G_n]$  to  $0_\chi[\Sigma_{n+e}]$  by mapping  $\sigma$  in  $G_n$  to  $\chi(\sigma)r_n(\sigma)$ , and extending by linearity. The image of (4.1) under this homomorphism is

$$\eta_n(c) = v_n(c)r_n(\xi_n) = \sum_{\sigma \in G_n} \delta_o(\sigma, c; M_n) \chi(\sigma)^{-1} r_n(\sigma)^{-1},$$

where  $v_n(c) = Nc - (c, F_{n+e}/F) \chi(c)$ . If  $m \geq n \geq n_0$ , Lemma 2.1 shows that the restriction map from  $G_m$  to  $G_n$  maps  $\xi_m$  to  $\xi_n$ , whence one sees easily that the  $\eta_n(c)$  ( $n \geq n_0$ ) define an element of  $\varprojlim_\leftarrow 0_\chi[\Sigma_{n+e}]$ . Let  $f_c(T, \chi)$  be the corresponding formal power series in the ring  $\Lambda_\chi = 0_\chi[[T]]$  under the isomorphism of Lemma 4.1. It is also clear that the  $v_n(c)$  ( $n \geq 0$ ) give an element of the same projective limit.

To see what the corresponding power series is, let  $\tau(c)$

in  $\mathbb{Z}_p$  be defined by the equation

$$(4.2) \quad (c, F_\infty/F) = \gamma_o^{\tau(c)},$$

where  $(c, F_\infty/F)$  is the element of  $\Gamma$  whose restriction to  $F_n$  is  $(c, F_n/F)$  for all  $n \geq 0$ . Then the  $v_n(c)$  ( $n \geq 0$ ) correspond to

$$(4.3) \quad u_c(T, \chi) = Nc - \chi(c) (1 + T)^{\tau(c)}$$

because the isomorphism of Lemma 4.1 maps  $\gamma_0$  to  $1 + T$ . Note that  $u_c(T, \chi)$  is not the zero power series since  $c \neq 1$ . We can therefore define  $G(T, \chi)$  in the quotient field of  $\Lambda_\chi$  by

$$(4.4) \quad G(T, \chi) = f_c(T, \chi)/u_c(T, \chi) \quad .$$

This ratio is independent of  $c$  because  $\eta_n(c)v_n(c') = \eta_n(c')v_n(c)$ , for any two ideals  $c, c'$ .

The next result gives an estimate for the denominator of  $G(T, \chi)$ . This estimate is probably best possible, but, at present, this is only known for  $F$  abelian over  $\mathbb{Q}$ . Recall that  $\theta$  is the character of  $G(M_0/F)$  giving its action on the group of  $q$ -th roots of unity. We say that  $\chi$  is exceptional if  $\chi\theta^{-1}$  is a character of  $F_e = F_\infty \cap M_0$ , i.e. if  $\chi\theta^{-1}$  is trivial on the subgroup of  $G(M_0/F)$  fixing  $F_e$ . If  $\chi$  is exceptional, we can associate with it a  $p^e$ -th root of unity  $\zeta_\chi$  by  $\zeta_\chi = \chi\theta^{-1}(\tilde{\gamma}_0)$ , where  $\tilde{\gamma}_0$  denotes the restriction of  $\gamma_0$  to  $F_e$ .

Theorem 4.2. Assume that the hypothesis  $D(p)$  is valid for  $F$ . Then (i) if  $\chi$  is not exceptional,  $G(T, \chi)$  belongs to  $\Lambda_\chi$ ; and (ii) if  $\chi$  is exceptional,  $(\zeta_\chi(1+T)-u)G(T, \chi)$  belongs to  $\Lambda_\chi$ .

Proof. Let  $h(T)$  be the greatest common divisor of all the  $u_c(T, \chi)$ . This exists because  $\Lambda_\chi$  is a unique factorization domain. Let  $\pi$  be a local parameter of  $\mathcal{O}_\chi$ . Choosing  $c$  so that  $\tau(c)$  is a unit in  $\mathbb{Z}_p$ , we see that  $\pi$  does not divide all the coefficients of  $u_c(T, \chi)$ , and so the same is true for  $h(T)$ . Thus, by the preparation theorem, we can assume that  $h(T)$  is either 1 or a distinguished polynomial.

Assuming the latter to be the case, let  $\alpha$  be any root of  $h(T)$  in  $\mathbb{C}_p$ . Since  $\alpha$  is a root of  $u_c(T, \chi)$ , a simple computation shows that we must have  $\chi\theta^{-1}(c) = (u/(1+\alpha))^{\tau(c)}$  for all  $c$ . As  $|\alpha|_p < 1$ , it follows easily that  $\chi$  must be exceptional, and that  $\alpha = \zeta_\chi^{-1}u - 1$ . Noting that each zero of  $u_c(T, \chi)$  is simple, this sketch of the proof of Theorem 4.2 is complete. For full details see [5].

#### 4.3. The p-adic L-functions

We use the same notation as in §4.2. Recall that, by

definition, the  $p$ -adic  $L$ -function  $L_p(\chi, s)$  of  $\chi$  is the continuous function from  $\mathbb{Z}_p \setminus \{1\}$  to  $\mathbb{C}_p$  satisfying  $L_p(\chi, s) = L_S(\chi, s)$  for all rational integers  $s \leq 0$  with  $s \equiv 1 \pmod{\delta}$ , where  $\delta$  denotes the degree of  $F(\mu_q)$  over  $F$ . Our aim is to prove that such functions exist by evaluating  $G(u^s - 1, \chi)$  at the integers  $s \leq 0$  (using the congruence  $C(p)$  below). We use the following lemma, which is an easy consequence of the continuity of the isomorphism in Lemma 4.1. Let

$$R = \varprojlim 0 \left[ \sum_n \right].$$

Lemma 4.3. Suppose  $\beta : R \rightarrow \mathbb{C}_p$  is a continuous homomorphism of  $\theta$ -algebras. If  $\xi \in R$ , let  $f(T)$  be the corresponding power series under the isomorphism of Lemma 4.1. Then  $\beta(\xi) = f(\beta(\gamma_0) - 1)$ .

We now introduce a congruence, which, as usual, has been proven for  $F = \mathbb{Q}$  or  $F$  real quadratic (see [3], [5]). Again Deligne and Ribet's work should establish it in general. If  $\mathfrak{f}$  is an integral ideal of  $F$ , we write  $M_{\mathfrak{f}}$  for the ray class field of  $F$  modulo  $\mathfrak{f}$ .

Hypothesis  $C(p)$ . Let  $b, c, \mathfrak{f}$  be integral ideals of  $F$  with

bc prime to  $\mathfrak{f}$ , and  $\mathfrak{f}$  divisible by all primes above  $p$ . Then, for each integer  $s \geq 0$ , we have

$$(4.5) \quad \delta_s(b, c; \mathfrak{f}) \equiv (Nbc)^s \delta_0(b, c; \mathfrak{f}) \pmod{(w_s(M_{\mathfrak{f}}) \mathbb{Z}_p)}.$$

Remark. This congruence has many equivalent formulations. We only mention one here. Assume that hypothesis  $D(p)$  is valid for  $F$ . Then  $C(p)$  is equivalent to the (seemingly weaker) assertion that, for each integer  $n \geq 0$ , there exists an integer  $m = m(n)$  such that (4.5) holds to the modulus  $p^n \mathbb{Z}_p$  provided  $\mathfrak{f}$  is divisible by  $p^m$ .

Theorem 4.4. Assume that hypotheses  $D(p)$  and  $C(p)$  are valid for  $F$ . Then, for each integer  $s \geq 0$ , we have  $G(u^{-s}-1, \chi) = L_S(\chi^{-1}\theta^{-s}, -s)$ . In particular, the  $p$ -adic  $L$ -function  $L_p(\chi, s)$  exists and is given by  $G(u^s - 1, \chi^{-1}\theta)$ .

Remark. The functional equation for the complex abelian  $L$ -functions of  $F$  shows that  $L_p(\chi, s)$  is identically zero unless  $\chi$  is the character of a totally real abelian extension of  $F$ .

Proof. If  $x$  is a unit in  $\mathbb{Z}_p$ , we can decompose it in the



form  $x = \omega(x) \langle x \rangle$ , where  $\langle x \rangle \equiv 1 \pmod{q}$  and  $\omega(x)$  is a root of unity. Recall that  $\kappa$  is the fundamental character giving the action of  $\Gamma$  on  $W$ . For each integer  $s$ , we can clearly extend the character  $\kappa^{-s}$  of  $\Gamma$  to a continuous homomorphism of  $\mathcal{O}_\chi$ -algebras from  $R_\chi = \varprojlim_{\leftarrow} \mathcal{O}_\chi \left[ \frac{\mathbb{Z}}{q_n} \right]$  to  $\mathbb{C}_p$ . We now apply Lemma 4.3 to this extension of  $\kappa^{-s}$ . We deduce easily that

$$f_c(u^{-s-1}, \chi) = \lim_{n \rightarrow \infty} \rho_n(c),$$

where

$$\rho_n(c) \equiv \sum_{b \bmod \mathfrak{f}_n} \delta_{\mathcal{O}}(b, c; \mathfrak{f}_n) \chi^{-1}(b) \langle Nb \rangle^s \pmod{(q_n \mathcal{O}_\chi)} ;$$

here  $\mathfrak{f}_n$  denotes the conductor of  $M_n$  over  $F$ , and  $b$  runs over a set of integral ideals representing the ray classes modulo  $\mathfrak{f}_n$ . Assuming that  $s \geq 0$ , and noting that  $Nb = \theta(b) \langle Nb \rangle$  and  $q_n$  divides  $w_1(M_{\mathfrak{f}_n})$ , we deduce from congruence (4.5) that

$$\rho_n(c) \equiv (Nc)^{-s} \sum_{b \bmod \mathfrak{f}_n} \delta_s(b, c; \mathfrak{f}_n) \chi_1(b) \pmod{(q_n \mathcal{O}_\chi)},$$

$$\text{where } \chi_1 = \chi^{-1} \theta^{-s}.$$

But, by Lemma 2.1, the right hand side of this last congruence has the same value for all  $n \geq n_0$ , and this value is plainly

$$(4.6) \quad (Nc - \chi_1^{-1}(c))(Nc)^{-s} L_S(\chi_1, -s).$$

In other words,  $f_c(u^{-s-1}, \chi)$  is given by (4.6). But the first factor in (4.6) is just  $u_c(u^{-s-1}, \chi)$ , and so the proof is complete.

## §5. The main conjecture

The main conjecture, which first arose in Iwasawa's [12] work when  $F = \mathbb{Q}$ , asserts that the power series constructed in §4 via Stickelberger elements (i.e. the p-adic abelian L-functions of  $F$ ) are in fact characteristic power series of the  $\Lambda$ -modules constructed algebraically in §1. If true, this would provide a much deeper description of these  $\Lambda$ -modules than the algebraic theory alone can provide. Also, as Iwasawa has remarked, the truth of the main conjecture would provide an analogue for totally real number fields of Weil's well known interpretation, in terms of l-adic representations, of the L-functions attached to curves over finite fields.

### 5.1. The main conjecture

Let  $F$  be a totally real number field,  $p$  an odd prime

number, and  $\theta$  the character giving the action of the Galois group of  $F = F(\mu_p)$  over  $F$  on the group of  $p$ -th roots of unity. Assuming hypotheses  $C(p)$  and  $D(p)$  for  $F$ , the construction of §4 gives elements  $G(T, \theta^i)$  of the quotient field of  $\Lambda$  attached to each character  $\theta^i$  of  $G(F/F)$ . In fact,  $G(T, \theta^i)$  is not identically zero if and only if  $i$  is odd (this is plain from Theorem 4.4 and the fact that the functional equation of the complex  $L$ -functions implies that, for all integers  $k$  and  $n > 1$ ,  $L_S(\theta^k, 1-n)$  is non-zero if and only if  $k$  and  $n$  have the same parity). Also, for  $i$  odd, Theorem 4.4 shows that

$$G(u^S - 1, \theta^i) = L_p(\theta^{1-i}, s),$$

where  $L_p(\theta^{1-i}, s)$  is the  $p$ -adic  $L$ -function of  $\theta^{1-i}$ . Let  $\delta$  denote the degree of  $F$  over  $F$ , and let  $H(T, \theta^i)$  be either  $G(T, \theta^i)$  or  $(1 + T - u) G(T, \theta)$  according as  $i$  is not or is congruent to 1 modulo  $\delta$ . Then, by Theorem 4.2,  $H(T, \theta^i)$  belongs to  $\Lambda$ .

On the other hand, for each odd integer  $i$ , let  $G_i(T)$  be the power series defined by equation (1.4) of §1, i.e.  $G_i((1 + T)^{-1} - 1)$  is a characteristic power series of  $\text{Hom}(e_i A_\infty, Q_p/Z_p)$ , where  $A_\infty$  is the  $p$ -primary subgroup of the ideal class group of  $F_\infty = F(W)$ .

Main conjecture. For each odd integer  $i$ , the ideals  $(H(T, \theta^i))$  and  $(G_i(T))$  in  $\Lambda$  are equal.

Remark. In making the conjecture, we have been assuming that hypotheses  $C(p)$  and  $D(p)$  hold for  $F$ . However, until the work of Deligne and Ribet [6] is finished, it is worth bearing in mind that the existence of the  $G(T, \theta^i)$  (satisfying the conclusions of Theorems 4.2 and 4.4) can be proven under weaker hypotheses. In fact, it suffices to assume that  $C(p)$  and  $D(p)$  hold for some totally real number field  $K \subset F$  such that  $F$  is abelian over  $K$  (the essential point being that  $F = F(\mu_p)$  is then still abelian over  $K$ ).

While there is considerable evidence in favour of the main conjecture, it should also be stressed that it has only been proven in a few special cases. We now mention some numerical examples where it is known to be true.

- (i)  $F = \mathbb{Q}$ , and  $p$  an odd prime number such that the class number of the maximal real subfield of  $\mathbb{Q}(\mu_p)$  is prime to  $p$ , e.g.  $p \leq 4001$  (see [12]);
- (ii)  $F = \mathbb{Q}(\sqrt{11})$ ,  $p = 7$ ;
- (iii)  $F = \mathbb{Q}(\sqrt{14})$ ,  $p = 5$ ;
- (iv)  $F = \mathbb{Q}(\sqrt{\Delta})$ ,  $p = 3$ , where  $\Delta$  is either prime to 3 or of the form  $3(3m + 1)$ , and where

the 3-primary subgroup of the ideal class group of  $\mathbb{Q}(\sqrt{-3\Delta})$  is cyclic (see [2] for the last three examples).

## 5.2. Non group-theoretic evidence for the main conjecture.

By Theorem 1.13,  $G_1(u^s - 1)/(u^s - u)$  has a simple pole at  $s = 1$  if and only if the  $p$ -adic regulator  $R_p$  of  $F$  does not vanish. Moreover, if  $R_p \neq 0$ , the residue at this pole has the same  $p$ -adic valuation as

$$\rho_p(F) = \frac{2^{d-1} h R_p}{\sqrt{\Delta}} \prod_{p \in S} (1 - (Np)^{-1}).$$

On the other hand, by Theorem 4.4, the  $p$ -adic zeta function  $\zeta_p(F, s)$  of  $F$  is given by

$$\zeta_p(F, s) = H(u^s - 1, \theta)/(u^s - u).$$

Thus the following theorem of Leopoldt [16] (which one hopes will be established for all totally real  $F$  in the future) is in accord with the main conjecture.

Theorem 5.1. Assume that  $F$  is abelian over  $\mathbb{Q}$ . Then  $\zeta_p(F, s)$  has a simple pole at  $s = 1$  with residue  $\rho_p(F)$ .

By the Weierstrass preparation theorem, each non-zero

element  $f$  of  $\Lambda$  can be expressed uniquely in the form  $f = p^\mu g v$ , where  $\mu \geq 0$ ,  $g$  is a distinguished polynomial, and  $v$  is a unit in  $\Lambda$ . We call the degree  $\lambda$  of  $g$  and the integer  $\mu$  the  $\lambda$  and  $\mu$  invariants, respectively, of  $f$ . We omit the proof of the following theorem, which is based on the analytic class number formula (see [14] for the proof in an important case).

Theorem 5.2. Assume that  $F$  is an abelian extension of a totally real field  $K$  such that hypotheses  $C(p)$  and  $D(p)$  are valid for  $K$  (e.g.  $K = \mathbb{Q}$  or  $K$  real quadratic). Then

$$\prod_{\substack{i=1 \\ (i,2)=1}}^{\delta} G_i(T) \text{ and } \prod_{\substack{i=1 \\ (i,2)=1}}^{\delta} H(T, \theta^i) \text{ have the same } \lambda \text{ and } \mu$$

invariants.

On the other hand, even when  $F = \mathbb{Q}$ , it does not seem possible at present to prove unconditionally that  $G_i(T)$  and  $H(T, \theta^i)$  have the same  $\lambda$  and  $\mu$  invariants for each odd integer  $i$ . However, it is an easy consequence of Theorems 1.13 and 5.1 that this is true for  $i = 1$ .

Theorem 5.3. If  $F$  is abelian over  $\mathbb{Q}$ , then  $G_1(T)$  and  $H(T, \theta)$

have the same  $\lambda$  and  $\mu$  invariants.

### 5.3. Group-theoretic evidence for the main conjecture

In these lectures, we only discuss group theoretic evidence for the main conjecture which can be proven using Stickelberger's theorem and its conjectural generalization. Nevertheless, it should be noted that Iwasawa [10] has given an interesting alternative approach when  $F = \mathbb{Q}$ , based on explicit reciprocity laws.

As before, let  $F = F(\mu_p)$ ,  $F_\infty = F(W)$ , and let  $F_n$  be the  $n$ -th layer of  $F_\infty/F$ . Put  $G_n = G(F_n/F)$ , and let  $A_n$  be the  $p$ -primary subgroup of the ideal class group of  $F_n$ . Assume that hypothesis  $D(p)$  is valid for  $F$ , and let  $\mathfrak{c}$  be an integral ideal of  $F$  prime to  $p$ . Then, if  $n$  is so large that all primes of  $F$  above  $p$  are ramified in  $F_n$ ,  $D(p)$  shows that

$$(5.1) \quad (N\mathfrak{c} - (c, F_n/F)) \alpha_0(F_n/F)$$

belongs to  $\mathbb{Z}_p[G_n]$ . Therefore, for  $n$  sufficiently large, we define  $I(F_n/F)$  to be the ideal of  $\mathbb{Z}_p[G_n]$  generated by the elements (5.1) as  $\mathfrak{c}$  ranges over all integral ideals of  $F$  prime to  $p$ . If the stronger hypothesis  $H_0$  of §2 is valid for  $F$ , it is true (but not quite obvious) that  $I(F_n/F)$  is



the ideal of  $\mathbb{Z}_p[G_n]$  which is generated by the elements of the ideal  $I_0(F_n/F)$  of  $\mathbb{Z}[G_n]$  defined in §2.

Theorem 5.4. Assume that (i) hypothesis  $D(p)$  is valid for  $F$ , and (ii)  $I(F_n/F)$  annihilates  $A_n$  for all sufficiently large  $n$ . Then, for each odd integer  $i$ ,  $H((1+T)^{-1} - 1, \theta^i)$  annihilates  $\text{Hom}(e_i A_{\infty, \mathbb{Q}_p} / \mathbb{Z}_p)$ .

Remark. When  $F = \mathbb{Q}$ , assumption (ii) of the theorem is, of course, a consequence of Stickelberger's theorem (Theorem 3.1). When  $F$  is abelian over  $\mathbb{Q}$ , it is very probable that one can deduce (ii) from Stickelberger's theorem for  $F_n/\mathbb{Q}$ , but the details do not seem to have been worked out (cf. [18]).

Proof. Let  $\Delta = G(F/F)$ ,  $\sum_n = G(F_n/F)$ , so that  $G_n \xrightarrow{\sim} \Delta \times \sum_n$ . Let  $r_n$  be the projection map from  $G_n$  onto  $\sum_n$ . Then we have the ring isomorphism

$$(5.2) \quad e_i \mathbb{Z}_p[G_n] \xrightarrow{\sim} \mathbb{Z}_p[\sum_n]$$

given by mapping  $e_i \sigma$  to  $\theta^i(\sigma) r_n(\sigma)$  for each  $\sigma \in G_n$ . Let  $\mathfrak{c}$  be an integral ideal of  $F$  prime to  $p$ . Then our hypotheses assert that, assuming  $n$  sufficiently large,

$$(Nc - (c, F_n/F)) \alpha_o(F_n/F)$$

annihilates  $A_n$ . By virtue of (5.2), we conclude that, in the notation of §4,

$$\eta_n(c) = \sum_{\sigma \in G_n} \delta_o(\sigma, c; F_n) \theta^{-i}(\sigma) r_n(\sigma)^{-1}$$

annihilates  $e_i A_n$ , and thus that

$$\eta_n^*(c) = \sum_{\sigma \in G_n} \delta_o(\sigma, c; F_n) \theta^{-i}(\sigma) r_n(\sigma)$$

annihilates  $\text{Hom}(e_i A_n, \mathbb{Q}_p/\mathbb{Z}_p)$ . Since

$$\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p) = \varprojlim \text{Hom}(e_i A_n, \mathbb{Q}_p/\mathbb{Z}_p),$$

we deduce that, if we put  $T^* = (1 + T)^{-1} - 1$ , then, in the notation of §4,

$$f_c(T^*, \theta^i) = u_c(T^*, \theta^i) G(T^*, \theta^i)$$

annihilates  $\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ . If  $i \not\equiv 1 \pmod{\delta}$ , we can plainly choose  $c$  so that  $u_c(T^*, \theta^i)$  is a unit in  $\Lambda$ . If  $i \equiv 1 \pmod{\delta}$ , it is also clear that  $u_c(T, \theta)$  is  $1 + T - u$  times a unit in  $\Lambda$ . This completes the proof. The next corollary was first remarked by Greenberg [8].

Corollary 5.5. Assume that (i) hypotheses  $C(p)$  and  $D(p)$  are valid for  $F$ , and (ii)  $I(F_n/F)$  annihilates  $A_n$  for all sufficiently large  $n$ . Then, for each odd integer  $i$ , every root of  $G_i(T)$  is a root of  $H(T, \theta^i)$ . In particular,  $G_i(u^{-n} - 1) \neq 0$  for each positive integer  $n$ .

Proof. Suppose that

$$\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \sim \bigoplus_{j=1}^{s_i} \Lambda/(h_j).$$

Then, by definition,  $G_i(T^*)$  is a unit in  $\Lambda$  times  $h = \prod_{j=1}^{s_i} h_j$ . Since  $H(T^*, \theta^i)$  annihilates the left hand side of (5.3), it follows that, for some integer  $a \geq 0$ ,  $p^a H(T^*, \theta^i)$  annihilates the right hand side. Thus each  $h_j$  ( $1 \leq j \leq s_i$ ) must divide  $p^a H(T^*, \theta^i)$ . It is now clear that each root of  $G_i(T)$  must also be a root of  $H(T, \theta^i)$ . The final assertion follows from Theorem 4.4 because  $L_S(\theta^k, -n) \neq 0$  when  $k$  and  $n > 0$  have opposite parity.

Theorem 5.6. Assume that (i) hypotheses  $C(p)$  and  $D(p)$  are valid for  $F$ , (ii)  $I(F_n/F)$  annihilates  $A_n$  for all sufficiently large  $n$ , and (iii)  $\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$  is pseudo-isomorphic to a quotient of  $\Lambda$  for each odd integer  $i$ .

Then the main conjecture is true for  $F$  and  $p$ .

Proof. It can be shown that a quotient of  $\Lambda$  has no non-trivial  $\Lambda$ -sub-module of finite cardinality. Thus, if  $g_i(T)$  is a characteristic power series of  $\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ , then hypothesis (iii) implies that  $\Lambda/(g_i)$  can be identified with a  $\Lambda$ -submodule of  $\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$  of finite index. Since  $H((1+T)^{-1} - 1, \theta^i)$  annihilates  $\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$  by Theorem 5.4, it follows that  $g_i(T)$  must divide  $H((1+T)^{-1} - 1, \theta^i)$  for each odd integer  $i$ , whence  $G_i(T)$  must divide  $H(T, \theta^i)$  for each odd integer  $i$ . Appealing to Theorem 5.2, we then conclude that the main conjecture is true for  $F$  and  $p$ .

Remark. Very little is known about assumption (iii) of Theorem 5.6. On the one hand, it has only been proven in a few cases (cf. §5.4). On the other hand, no counter example is known to it.

#### 5.4. Proof of the main conjecture in special cases.

All proofs of the main conjecture in special cases depend on showing that hypotheses like (ii) and (iii) of

Theorem 5.6 are valid. Of course, (ii) is essentially equivalent to knowing Stickelberger's theorem for the abelian extensions  $F_n$  of  $F$ .

We now discuss a sufficient condition of the validity of (iii), when  $F = \mathbb{Q}$ , due to Greenberg [7]. Let  $J$  denote the element of  $G_\infty = G(F_\infty/F)$  defined by complex conjugation ( $J$  is independent of the particular embedding we take of  $F_\infty$  in  $\mathbb{C}$ ). Since  $p$  is odd, we have  $A_\infty = A_\infty^+ \oplus A_\infty^-$ , where

$$A_\infty^+ = A_\infty^{1+J} = \bigoplus_{\substack{i=1 \\ i \text{ even}}}^{\delta} e_i A_\infty, \quad A_\infty^- = A_\infty^{1-J} = \bigoplus_{\substack{i=1 \\ i \text{ odd}}}^{\delta} e_i A_\infty.$$

Note that the main conjecture is only concerned with describing the dual of  $A_\infty^-$  in terms of  $p$ -adic  $L$ -functions.

Theorem 5.7. Assume that  $F = \mathbb{Q}$ , and that  $A_\infty^+ = 0$ . Then the main conjecture is true for  $F$  and  $p$ .

Proof. By Theorem 5.6, we must show that  $A_\infty^+ = 0$  implies condition (iii) of Theorem 5.6. The way in which we use  $A_\infty^+ = 0$  is the following. Let  $E_\infty$  be the group of units of the ring of integers of  $F_\infty$ . Let  $N_\infty$  be the field obtained

by adjoining to  $F_\infty$  the  $p^n$ -th ( $n = 1, 2, \dots$ ) roots of all elements of  $E_\infty$ . Obviously,  $N_\infty$  is contained in  $M_\infty$ , the maximal abelian  $p$ -extension of  $F_\infty$  which is unramified outside the primes above  $p$ . As before, put  $X_\infty = G(M_\infty/F_\infty)$ . Then  $J \in G_\infty$  acts on  $X_\infty$  in the manner explained in §1, and, since  $p \neq 2$ , we have  $X_\infty = X_\infty^+ \oplus X_\infty^-$ . Define  $M_\infty^-$  to be the fixed field of  $X_\infty^+$ , so that  $G(M_\infty^-/F_\infty) = X_\infty^-$ . Then  $A_\infty^+ = 0$  implies that

$$(5.3) \quad M_\infty^- = N_\infty.$$

Indeed, by Kummer theory (cf. Theorem 1.9), (5.3) is equivalent to  $V_\infty^+ = (\mathbb{Q}_p/\mathbb{Z}_p) \otimes E_\infty$ , and this latter equation is equivalent to  $A_\infty^+ = 0$  by virtue of Lemma 1.10. Now assume that  $F = \mathbb{Q}$ . Then, since there is only one prime of  $F_\infty$  above  $p$ , Iwasawa ([13], Theorem 15) has shown that  $G(N_\infty/F_\infty) \sim \Lambda^{r_2(\bar{F})}$ . Moreover, since  $F = \mathbb{Q}$ , one deduces easily from the proof of Theorem 15 in [13], or from the proof of Theorem 1.8 sketched earlier, that in fact  $e_i G(N_\infty/F_\infty) \sim \Lambda$  for each odd integer  $i \bmod (p-1)$ . In addition, it is also shown in [13] that  $G(N_\infty/F_\infty)$  has no non-trivial finite  $\Lambda$ -submodule, so that  $e_i G(N_\infty/F_\infty)$  can be embedded in  $\Lambda$  as a submodule of finite index for each odd  $i$ . Now let  $L_\infty$  be the maximal unramified abelian  $p$ -extension of  $F_\infty$ ,

and let  $L_{\infty}^{-}$  be the fixed field of  $G(L_{\infty}/F_{\infty})^{+}$ . By (5.3), we have  $L_{\infty}^{-} \subset N_{\infty}$ , and so, for each odd integer  $i$ ,  $e_i G(L_{\infty}/F_{\infty}) = e_i G(L_{\infty}^{-}/F_{\infty})$  is a quotient of  $e_i G(N_{\infty}/F_{\infty})$ . We conclude easily that  $e_i G(L_{\infty}/F_{\infty})$  is pseudo-isomorphic to a quotient of  $\Lambda$ . The proof of Theorem 5.7 is now complete, since it is known ([13], Theorem 11) that  $e_i G(L_{\infty}/F_{\infty}) \sim \text{Hom}(e_i A_{\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$ .

Corollary 5.8. Assume that the class number of the maximal real subfield of  $\mathbb{Q}(\mu_p)$  is prime to  $p$ . Then the main conjecture is true for  $\mathbb{Q}$  and  $p$ .

Indeed, it is known [10] that the hypothesis of the corollary implies that the class number of the maximal real subfield of  $\mathbb{Q}(\mu_{n+1})$  is prime to  $p$  for all  $n \geq 0$ , whence certainly  $A_{\infty}^{+} = 0$ .

Remarks. (i) In all numerical cases computed so far, the class number of the maximal real subfield of  $\mathbb{Q}(\mu_p)$  has been prime to  $p$ . (ii). At present, we know of no example of a totally real number field  $F$  and an odd prime  $p$  for which it can be proven that  $A_{\infty}^{+} \neq 0$  (cf. [7]). (iii). If  $F$  is any totally real number field, and  $p$  an odd prime, it would be



interesting to know whether  $A_{\infty}^{+} = 0$  implies that  $\text{Hom}(e_i A_{\infty}, \mathbb{Q}_p / \mathbb{Z}_p)$  is pseudo-isomorphic to a quotient of  $\Lambda$  for each odd  $i$ .

Finally, we mention without proof another theorem, proven in [2], which gives sufficient conditions for the main conjecture to hold. Let  $A_0$  be the  $p$ -primary subgroup of the ideal class group of  $F$ .

Theorem 5.9. Assume that  $F$  is abelian over  $\mathbb{Q}$ , and that (i)  $A_0^{-}$  is cyclic over  $\mathbb{Z}_p[G(F/\mathbb{Q})]$ , (ii) no prime of the maximal real subfield of  $F$  above  $p$  splits in  $F$ , and (iii)  $p$  does not divide  $[F:\mathbb{Q}]$ . Then the main conjecture is true for  $F$  and  $p$ .

Examples (ii), (iii), (iv) given after the main conjecture are all special cases of this theorem.

### 5.5. Consequences of the main conjecture

Again let  $F$  be totally real, and  $p$  an odd prime. Birch and Tate when  $n = 1$ , and Lichtenbaum for all odd  $n \geq 1$ , have conjectured that the exact power of  $p$  dividing

$w_{n+1}(F) \zeta(F, -n)$  is equal to the order of a certain K-group and a certain étale cohomology group associated with  $F$ , respectively. We do not go into the background of these conjectures. Instead, we simply give an equivalent formulation of these conjectures in terms of the Iwasawa modules discussed in these notes.

Let  $M$  be a  $\mathbb{Z}_p$ -module, which is also a module for  $G_\infty = G(F_\infty/F)$ , and let  $T = \varprojlim_p \mu_{p^n}$  be the Tate module. For each integer  $n > 0$ , we define  $M(n)$  to be the  $G_\infty$ -module

$$M(n) = M \otimes_{\mathbb{Z}_p} T \otimes_{\mathbb{Z}_p} \dots \otimes_{\mathbb{Z}_p} T \quad (n \text{ times}),$$

where  $M(n)$  is endowed with the diagonal action of  $G_\infty$ .

Conjecture 5.10. For each odd positive integer  $n$ , the group  $(A_\infty^-(n))^{G_\infty}$  is finite, and its order is equal to the exact power of  $p$  dividing  $w_{n+1}(F) \zeta(F, -n)$ .

Theorem 5.11. The main conjecture implies Conjecture 5.10.

To see this, we combine the next lemma with Theorem 4.4 and the fact that, up to a unit, the power of  $p$  dividing  $w_{n+1}(F)$  is either 1 or  $u^{-n} - u$ , according as  $n+1$  is not or is

divisible by  $\delta$ , where  $\delta = [F:F]$ .

Lemma 5.12. Let  $n$  be an odd positive integer such that  $n \equiv -i \pmod{\delta}$ . Then (i)  $(A_{\infty}^{-}(n))^{G_{\infty}}$  is finite if and only if  $G_i(u^{-n} - 1) \neq 0$ , and (ii) if  $G_i(u^{-n} - 1) \neq 0$ , then the order of  $(A_{\infty}^{-}(n))^{G_{\infty}}$  is equal to the power of  $p$  dividing  $G_i(u^{-n} - 1)$ .

This lemma is an easy consequence of Lemma 9 of Appendix 1, and the fact ([13], Theorem 18) that  $\text{Hom}(e_i A_{\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$  has no non-trivial finite  $\Lambda$ -submodule.

We conclude by mentioning some evidence for conjecture 5.10, which is valid unconditionally.

Theorem 5.13. Assume that  $F$  is abelian over  $\mathbb{Q}$ . Let  $n$  be an odd positive integer with  $n \equiv -1 \pmod{\delta}$ . Then  $(A_{\infty}^{-}(n))^{G_{\infty}} \neq 0$  if and only if  $p$  divides  $w_{n+1}(F) \zeta(F, -n)$ .

Proof. We first note that, by Theorems 1.13 and 5.1,  $G_1(u - 1)$  and  $H(u - 1, \theta)$  are divisible by the same power of  $p$ , and so one is a unit if and only if the other is. Now, by Lemma 5.12,  $(A_{\infty}^{-}(n))^{G_{\infty}}$  is trivial if and only if

$G_1(u^{-n} - 1)$  is a unit. But  $G_1(u^{-n} - 1)$  is congruent to  $G_1(u - 1) \bmod p$ , and similarly  $H(u^{-n} - 1, \theta)$  is congruent to  $H(u - 1, \theta) \bmod p$ . The assertion of the theorem now follows because Theorem 4.4 shows that  $H(u^{-n} - 1, \theta)$  is  $w_{n+1}(F) \zeta(F, -n)$  times a unit in  $\mathbb{Z}_p$ .

There would be great interest in proving Theorem 5.13 unconditionally for other congruence classes of  $n \bmod \delta$ , even when  $F = \mathbb{Q}$ . We give a more down to earth formulation of the problem. Let  $A_0$  be the  $p$ -primary subgroup of the ideal class group of  $F$ .

Lemma 5.14. Assume that no prime of the maximal real subfield of  $F$  lying above  $p$  splits in  $F$ . Then, for each odd positive integer  $n$ ,  $(A_\infty^-(n))^{G_\infty} \neq 0$  if and only if the component  $e_{-n} A_0^-$  of  $A_0^-$  is non-trivial.

Proof. Let  $\Gamma = G(F_\infty/F)$ . It is known ([2], Theorem 2.6) that the hypothesis of the lemma is equivalent to the existence of an isomorphism  $A_0^- \xrightarrow{\sim} (A_\infty^-)^\Gamma$ . Granted this, the lemma follows from the fact that a discrete  $\Gamma$ -module is trivial if and only if its group of  $\Gamma$ -invariants is trivial,

and the observation that  $(A_{\infty}^{-}(n))^{\Delta} = (e_{-n}A_{\infty}^{-})(n)$ .

Thus, in the case  $F = \mathbb{Q}$ , we are left with the following classical problem on cyclotomic fields. Let  $n$  be an odd integer satisfying  $1 < n < p - 2$ . Is it true that  $p$  divides  $\zeta(\mathbb{Q}, -n)$  if and only if  $e_{-n}A_{\infty}^{-} \neq 0$ ? One implication is well known (see [2], Theorem 2.5) and classical, but it has never been proven unconditionally that  $p$  divides  $\zeta(\mathbb{Q}, -n)$  implies that  $e_{-n}A_{\infty}^{-} \neq 0$ .<sup>†</sup>

### Appendix 1.

The aim of this appendix is to give the proof of Theorem 1.13. Throughout  $p$  will denote an odd prime number,  $\Psi_n$  the  $n$ -th layer of the cyclotomic  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}_p$ , and  $V_n$  the units of  $\Psi_n$  which are  $\equiv 1$  modulo the maximal ideal. Let  $N_n$  denote the norm map from  $\Psi_n$  to  $\mathbb{Q}_p$ . Put  $V = V_0$ .

Lemma 1. For each  $n \geq 0$ , we have  $N_n(V_n) = V^{p^n}$ .

Proof. The lemma in fact remains true if we replace  $\Psi_n$  by any totally ramified abelian extension of  $\mathbb{Q}_p$  of degree  $p^n$  over  $\mathbb{Q}_p$ , as the following argument shows. Pick a local

---

<sup>†</sup> See note added in proof.

parameter  $\pi_n$  in  $\Psi_n$ . Since  $\Psi_n/\mathbb{Q}_p$  is totally ramified,  $\tau_n = N_n(\pi_n)$  is a local parameter in  $\mathbb{Q}_p$ . Thus we have

$$\Psi_n^\times = \mu_{p-1} \times \{\pi_n\} \times V_n, \quad \mathbb{Q}_p^\times = \mu_{p-1} \times \{\tau_n\} \times V, \quad ,$$

where  $\{\pi_n\}$ ,  $\{\tau_n\}$  are the cyclic groups generated by  $\pi_n$ ,  $\tau_n$ , respectively. Now, by local class field theory, the index of  $N_n(\Psi_n^\times)$  in  $\mathbb{Q}_p^\times$  is  $p^n$ . Since  $N_n(\mu_{p-1}) = \mu_{p-1}$ , and  $N_n(\{\pi_n\}) = \{\tau_n\}$  by construction, we must therefore have  $N_n(V_n) = V^{p^n}$ . This completes the proof.

We use the notation of §1, taking  $F$  to be an arbitrary totally real finite extension of  $\mathbb{Q}$ . Again  $S$  will denote the set of primes of  $F$  above  $p$ . For each  $p \in S$ ,  $U_{p,1}$  will denote the units in the completion of  $F$  at  $p$  which are  $\equiv 1 \pmod{p}$ , and we put

$$U_1 = \prod_{p \in S} U_{p,1} \quad .$$

For each  $n \geq 0$ ,  $F_n$  denotes the  $n$ -th layer of the cyclotomic  $\mathbb{Z}_p$ -extension  $F_\infty$  of  $F$ , and we write  $C_n$  for the idèle class group of  $F_n$  (we write  $C$  for  $C_0$ ). Let  $N_{F_n/F}$  be the norm map from  $C_n$  to  $C$ , and put

$$Y = \bigcap_{n \geq 0} N_{F_n/F} C_n \quad .$$

We view  $U_1$  as being embedded in  $C$  in the usual way, and

identify it with its image. Let  $N_{F/Q}$  be the map from  $U_1$  to  $V$  given by the product of the local norms at the  $p \in S$ .

Finally, if  $L/K$  is an abelian extension of local or global fields, and  $\xi$  belongs to  $K^\times$  or the idèle class group of  $K$  according as  $K$  is local or global, we denote the Artin symbol of  $\xi$  for  $L/K$  by  $(\xi, L/K)$ .

Lemma 2.  $Y \cap U_1$  is the kernel of  $N_{F/Q}$ .

Proof. Recall that  $\mathbb{Q}_\infty$  denotes the cyclotomic  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$ . Define the integer  $e \geq 0$  by  $\mathbb{Q}_\infty \cap F = \mathbb{Q}_e$ . Thus, for each  $n \geq 0$ ,  $F_n = F \mathbb{Q}_{n+e}$ . Suppose first that  $\xi \in Y \cap U_1$ . Since  $\xi \in N_{F_n/F} C_n$ , we have  $(\xi, F_n/F) = 1$  for each  $n \geq 0$ . Restricting this Artin symbol to  $\mathbb{Q}_{n+e}$ , and recalling that there is only one prime of  $\mathbb{Q}_{n+e}$  above  $p$ , it follows that  $N_{F/Q} \xi$  is a norm from  $\Psi_{n+e}$ ; clearly it must then be a norm from  $V_{n+e}$ . Hence, by Lemma 1,  $N_{F/Q} \xi \in V^{p^{n+e}}$  for all  $n \geq 0$ , and so  $N_{F/Q} \xi = 1$ . Conversely let  $\xi$  be an element of  $U_1$  with  $N_{F/Q} \xi = 1$ . Let  $N_{F/Q_e}$  be the map from  $U_1$  to  $V_e$  given by the product of the local norms at the  $p \in S$ , and put  $\beta = N_{F/Q_e} \xi$ . By class field theory,  $(\beta, \Psi_{n+e}/\Psi_e) = (N_e \beta, \Psi_{n+e}/\mathbb{Q}_p)$ , both Artin symbols being viewed as elements



of  $G(\Psi_{n+e}/\mathbb{Q}_p)$ . Since  $N_e \beta = 1$ , it follows that

$$(\beta, \Psi_{n+e}/\Psi_e) = (\beta, \mathbb{Q}_{n+e}/\mathbb{Q}_e) = 1$$

for all  $n \geq 0$ . But the restriction map from  $G(F_n/F)$  to  $G(\mathbb{Q}_{n+e}/\mathbb{Q}_e)$  is injective, and so  $(\xi, F_n/F) = 1$ , i.e.

$\xi \in N_{F_n/F}^C$  for  $n \geq 0$ . This completes the proof.

Lemma 3. Let  $L$  be the  $p$ -Hilbert class field of  $F$ . Let the integers  $e$  and  $k \geq 0$  be defined by  $F \cap \mathbb{Q}_\infty = \mathbb{Q}_e$  and  $L \cap F_\infty = F_k$ . Then  $N_{F/\mathbb{Q}}(U_1) = v^{e+k}$ .

Proof. For each prime  $q$  of  $F_n$  above  $p$ , let  $U_{q,1}(n)$  be the units  $\equiv 1 \pmod{q}$  in the completion of  $F_n$  at  $q$ . Then, with  $k$  as defined in the statement of the lemma, the norm map from  $U_1(k) = \prod_{q|p} U_{q,1}(k)$  to  $U_1$  is surjective. This is because  $F_k/F$  is unramified, and the norm map for an unramified extension of local fields is surjective on the units (and so also surjective when restricted to the units  $\equiv 1$ ). It follows that

$$N_{F/\mathbb{Q}}(U_1) = N_{F_k/\mathbb{Q}}(U_1(k)) .$$

But, as  $F_k$  contains  $\mathbb{Q}_{k+e}$ , the group on the right is

contained in  $N_{k+e}(V_{k+e}) = V^{p^{k+e}}$ . Therefore  $N_{F/\mathbb{Q}}(U_1)$ , being a closed subgroup of finite index of  $V$ , is of the form  $V^{p^r}$ , where  $r \geq e + k$ . We now proceed to show that we must have  $r = e + k$ . We do this by showing that every element of  $G(F_{r-e}/F_k)$  is 1. Let  $\sigma$  be any element of  $G(F_{r-e}/F_k)$ , and put  $t = r - e$ . Since  $L \cap F_t = F_k$ , there exists  $\tau \in G(LF_t/L)$  whose restriction to  $F_t$  is  $\sigma$ . As  $\tau$  fixes  $L$ , class field theory shows that there exists  $\xi \in U_1$  such that  $(\xi, LF_t/F) = \tau$ , whence  $(\xi, F_t/F_k) = \sigma$ . Now, since the restriction map from  $G(F_t/F_k)$  to  $G(\mathbb{Q}_r/\mathbb{Q}_{k+e})$  is injective, it suffices to show that the restriction of  $\sigma$  to  $\mathbb{Q}_r$  is 1. But this restriction is  $(N_{F/\mathbb{Q}}\xi, \mathbb{Q}_r/\mathbb{Q})$ , and this is certainly 1 because, by hypothesis,  $N_{F/\mathbb{Q}}\xi$  belongs to  $V^{p^r} = N_r(V_r)$ . Thus  $\sigma$  is indeed 1, and the proof is complete.

We now make some index computations. For each  $p \in S$ , let  $F_p$  be the completion of  $F$  at  $p$ ,  $\mathcal{O}_p$  the ring of integers of  $F_p$ , and  $e_p$  the ramification index of  $F_p$  over  $\mathbb{Q}_p$ . Choose an integer  $t \geq 0$  such that  $p^{-t} \mathcal{O}_p$  contains  $\log U_{p,1}$  for each  $p \in S$ , where  $\log$  denotes the  $p$ -adic logarithm. Define

$$\Omega = \prod_{p \in S} p^{-t} \theta_p, \quad \log U_1 = \prod_{p \in S} \log U_{p,1}.$$

For  $p \in S$ , let  $v_p$  denote the order of the group of  $p$ -power roots of unity in  $F_p$ . Recall that  $d = [F:\mathbb{Q}]$ .

Lemma 4.  $[\Omega : \log U_1] = p^{td} \prod_{p \in S} (v_p Np)$ .

Proof. Fix  $p \in S$ . The kernel of the logarithm map on  $U_{p,1}$  is the group of  $p$ -power roots of unity of  $F_p$ . On the other hand, if we define  $r = [e_p/(p-1)] + 1$ , and let  $U_{p,r}$  denote the units  $\equiv 1 \pmod{p^r}$ , then the restriction of the logarithm to  $U_{p,r}$  defines an isomorphism from  $U_{p,r}$  onto  $p^r$ . Therefore the kernel of the map from  $U_{p,1}/U_{p,r}$  onto  $(\log U_{p,1})/(\log U_{p,r})$ , which is induced by the logarithm, can be identified with the group of  $p$ -power roots of unity in  $F_p$ . Thus

$$[\log U_{p,1} : p^r] = (Np)^{r-1}/v_p,$$

whence

$$[p^{-t} \theta_p : \log U_{p,1}] = (Np)^{1+te_p} v_p.$$

Taking the product over all  $p \in S$ , and recalling that

$$\prod_{p \in S} (Np)^{e_p} = p^d, \quad \text{the assertion of the lemma follows.}$$

Let  $E_1$  be the group of global units of  $F$  which are  $\equiv 1 \pmod{p}$  for each  $p \in S$ . Since  $F$  is totally real and  $p \neq 2$ , Dirichlet's theorem shows that  $E_1$  is a free  $\mathbb{Z}$ -module of rank  $d - 1$ . Let  $\phi : F \rightarrow \prod_{p \in S} F_p$  be the canonical embedding. We define  $D$  to be the  $\mathbb{Z}_p$ -submodule of  $U_1$  which is generated by  $\phi(E_1)$  and  $\phi(\varepsilon_d)$ , where  $\varepsilon_d = 1 + p$ . We write  $\log D$  for the subset of  $\log U_1$  which is obtained by applying the  $p$ -adic logarithm to each component of the vectors in  $D$ .

Lemma 5. The index of  $\log D$  in  $\log U_1$  is finite if and only if the  $p$ -adic regulator  $R_p$  of  $F$  is non-zero. If  $R_p \neq 0$ , then  $[\log U_1 : \log D]$  is equal to the inverse of the  $p$ -adic valuation of

$$\frac{d_p R_p}{\sqrt{\Delta}} \prod_{p \in S} (v_p Np)^{-1}.$$

Proof. For  $p \in S$ , let  $\phi_p$  be the canonical embedding of  $F$  in  $F_p$ ,  $d_p = [F_p : \mathbb{Q}_p]$ , and  $\alpha_1^{(p)}, \dots, \alpha_{d_p}^{(p)}$  a  $\mathbb{Z}_p$ -basis of  $\mathcal{O}_p$ . If  $\varepsilon_1, \dots, \varepsilon_{d-1}$  are a  $\mathbb{Z}$ -basis of  $E_1$ , we have

$$(1) \quad \log \phi_p(\varepsilon_j) = \sum_{k=1}^{d_p} a_{jk}^{(p)} p^{-t} \alpha_k^{(p)},$$

where the  $a_{jk}^{(p)}$  belong to  $\mathbb{Z}_p$ . Let  $A$  be the  $d \times d$  matrix formed from the  $a_{jk}^{(p)}$  ( $1 \leq j \leq d$ ,  $1 \leq k \leq d_p$ ,  $p \in S$ ). Then the index of  $\log D$  in  $\Omega$  is either infinite or finite and equal to the exact power of  $p$  dividing  $\det A$ , according as  $\det A$  is or is not 0. To compute  $\det A$ , let  $\phi_j$  ( $1 \leq j \leq d$ ) run through the distinct embeddings of  $F$  in the algebraic closure of  $\mathbb{Q}_p$ , and  $\sigma_j^{(p)}$  ( $1 \leq j \leq d_p$ ) through the distinct embeddings of  $F_p$  in the algebraic closure of  $\mathbb{Q}_p$ . Let  $E_p$  be the  $d \times d$  matrix formed from the  $\sigma_j^{(p)} \alpha_k^{(p)}$  ( $1 \leq j, k \leq d_p$ ), and let  $E$  be the direct sum of the  $E_p$ ,  $p \in S$  (i.e. the  $d \times d$  matrix with the blocks  $E_p$  ( $p \in S$ ) down the diagonal, and zeros outside these blocks). Let  $\Theta$  be the  $d \times d$  matrix formed from the  $\log \phi_k(\epsilon_j)$  ( $1 \leq j, k \leq d$ ). It follows from (1) that  $\Theta = A E$ . But  $\det \Theta = (d \log \epsilon_d) R_p(1)$ , where  $R_p(1)$  is the  $p$ -adic regulator of  $E_1$  (see, for example, [14]). Also the power of  $p$  occurring in  $(\det E_p)^2$  is  $p^{-2td_p}$  times the discriminant of  $F_p$  over  $\mathbb{Q}_p$ . Thus, using the standard relation between local and global discriminants, the power of  $p$  dividing  $(\det E)^2$  is  $p^{-2td}$  times the  $p$ -part of the discriminant  $\Delta$  of  $F$  over  $\mathbb{Q}$ . The first assertion of the lemma is now plain since  $\log U_1$  has finite index in  $\Omega$ .

Moreover, assuming  $R_p \neq 0$ , and recalling that  $R_p$  and  $R_p(1)$  have the same  $p$ -adic valuation because the index of  $E_1$  in the group of all units is prime to  $p$ , it follows that

$$[\Omega : \log D] = |d \log(\varepsilon_d) p^{td} R_p / \sqrt{\Delta}|_p^{-1}.$$

Noting that the  $p$ -adic valuation of  $\log \varepsilon_d$  is  $p^{-1}$ , the assertion of the lemma now follows from Lemma 4.

Lemma 6. The index of  $D$  in  $U_1$  is finite if and only if  $R_p \neq 0$ . If  $R_p \neq 0$ , then  $[U_1 : D]$  is equal to the inverse of the  $p$ -adic valuation of

$$\frac{d p R_p}{\sqrt{\Delta}} \prod_{p \in S} (Np)^{-1}.$$

Proof. The first assertion is plain. Assuming  $R_p \neq 0$ , it follows that  $D$  has no torsion. Thus the kernel of the map from  $U_1/D$  to  $\log U_1/(\log D)$  induced by the logarithm is the same as the kernel of the logarithm on  $U_1$ . Since this latter kernel has order  $\prod_{p \in S} v_p$ , the conclusion of Lemma 6 is clear from Lemma 5.

The  $\mathbb{Z}_p$ -submodule of  $U_1$  which is generated by  $\phi(E_1)$  is, of course, simply the closure  $\overline{\phi(E_1)}$  of  $\phi(E_1)$  in  $U_1$  in the

p-adic topology. Since  $p \neq 2$ , it follows from Lemma 2 that  $\overline{\phi(E_1)}$  is contained in  $Y \cap U_1$ . Recall that  $L$  is the p-Hilbert class field of  $F$ .

Lemma 7. The index of  $\overline{\phi(E_1)}$  in  $Y \cap U_1$  is finite if and only if  $R_p \neq 0$ . If  $R_p \neq 0$ , this index is equal to the inverse of the p-adic valuation of

$$w_1(F(\mu_p)) R_p p^k \prod_{p \in S} (1 - (Np)^{-1}) / \sqrt{\Delta} \quad ,$$

where  $k$  is defined by  $F_\infty \cap L = F_k$ .

Proof. The first assertion is plain, and so we assume that  $R_p \neq 0$ . It is clear from Lemma 2 that

$$(2) \quad D \cap Y = \overline{\phi(E_1)} \quad .$$

In particular, this implies that the natural map from  $Y \cap U_1 / \overline{\phi(E_1)}$  to  $U_1 / D$  is injective. Therefore, by the snake lemma, we have

$$(3) \quad [Y \cap U_1 : \overline{\phi(E_1)}] = [U_1 : D] / \#(B_1/B_2),$$

where  $B_1 = U_1 / (Y \cap U_1)$  and  $B_2 = D / \overline{\phi(E_1)}$ . Also, it is evident that

$$N_{F/\mathbb{Q}}(D) = N_{F/\mathbb{Q}}(\varepsilon_d^{\mathbb{Z}_p}) = v^d \quad .$$



Moreover, by Lemma 3, we have the commutative diagram with exact rows

$$\begin{array}{ccccccc}
 0 & \longrightarrow & Y \cap U_1 & \longrightarrow & U_1 & \xrightarrow{N_{F/Q}} & V^{p^{e+k}} \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & \overline{\phi(E_1)} & \longrightarrow & D & \xrightarrow{N_{F/Q}} & V^d \longrightarrow 0 .
 \end{array}$$

Since the vertical map on the extreme right is injective by (2), we conclude from the snake lemma that

$$(4) \quad \#(B_1/B_2) = |p^{e+k}/d|_p^{-1} .$$

Combining (3) and (4), and noting that  $p^{e+1}$  is just the  $p$ -part of  $w_1(F(\mu_p))$ , Lemma 7 now follows from Lemma 6.

As in §1, let  $M$  be the maximal abelian  $p$ -extension of  $F$  which is unramified outside  $S$ .

Lemma 8.  $G(M/F_\infty)$  is finite if and only if  $R_p \neq 0$ . If  $R_p \neq 0$ , the order of  $G(M/F_\infty)$  is given by the inverse of the  $p$ -adic valuation of

$$w_1(F(\mu_p)) \cdot h_{R_p} \prod_{p \in S} (1 - (Np)^{-1}) / \sqrt{\Delta} .$$

Proof. Let  $\psi$  be the Artin map from  $C$  onto  $G(M/F)$ . By

class field theory,  $\psi$  maps  $U_1$  onto  $G(M/L)$ , and the kernel of  $\psi$  restricted to  $U_1$  is precisely  $\overline{\phi(E_1)}$ . In addition, if  $\xi \in C$ , then  $\psi(\xi)$  fixes  $F_\infty$  if and only if  $\xi$  is in  $Y$ . Thus, as  $Y \cap \overline{\phi(E_1)} = \overline{\phi(E_1)}$  by Lemma 2, it follows that  $\psi$  induces an isomorphism

$$Y \cap U_1 / \overline{\phi(E_1)} \xrightarrow{\sim} G(M/LF_\infty) .$$

Since

$$\#(G(LF_\infty/F_\infty)) = \#(G(L/F_\infty \cap L)) = |h/p^k|_p^{-1} ,$$

Lemma 8 follows from Lemma 7.

Finally, we record, without proof, the following elementary lemma on  $\Lambda$ -modules (for the proof of a slightly easier result, see [2], p. 538). If  $B$  is a  $\Lambda$ -module, we write  $B^\Gamma$ ,  $B_\Gamma$  for the kernel and cokernel, respectively, of multiplication by  $T$  on  $B$ .

Lemma 9. Suppose that  $B \sim \bigoplus_{j=1}^r \Lambda/(h_j)$ , where  $h = \prod_{j=1}^r h_j \neq 0$ . Then the following three assertions are equivalent:- (i)  $B_\Gamma$  is finite, (ii)  $B^\Gamma$  is finite, and (iii)  $h(0) \neq 0$ . If these three assertions hold, then

$$\#(B_\Gamma) / \#(B^\Gamma) = |h(0)|_p^{-1} .$$

We can now complete the proof of Theorem 1.13. Recall that  $M_\infty$  is the maximal abelian  $p$ -extension of  $F_\infty$ , which is unramified outside the primes of  $F_\infty$  above  $p$ . Let  $M_\infty$  be the analogous field for  $F_\infty$ , i.e.  $M_\infty$  is the maximal abelian  $p$ -extension of  $F_\infty$ , which is unramified outside the primes of  $F_\infty$  above  $p$ . As in §1,  $X_\infty = G(M_\infty/F_\infty)$ , and we put  $X_\infty = G(M_\infty/F_\infty)$ . Since the degree of  $F_\infty/F_\infty$  is prime to  $p$ , one sees easily that

$$(5) \quad e_o X_\infty = G(M_\infty F_\infty / F_\infty) \xrightarrow{\sim} X_\infty.$$

But  $X_\infty$  is  $\Lambda$ -torsion by Theorem 1.8, whence  $e_o X_\infty$  is  $\Lambda$ -torsion. Therefore, by (1.1) of §1, we have

$$e_o X_\infty \sim \bigoplus_{j=1}^{r_o} \Lambda / (f_{jo}) \quad , \quad \text{where} \quad f_o(T) = \prod_{j=1}^{r_o} f_{jo}(T).$$

Also, by the definition of  $G_1(T)$  (see (1.4) of §1), we have  $f_o(0) = G_1(u-1)$ . Now, as remarked just prior to Theorem 1.6,

$$(6) \quad (X_\infty)_\Gamma = G(M/F_\infty).$$

Combining (5), (6) and Lemmas 8 and 9, we conclude that

$G_1(u-1) \neq 0$  if and only if  $R_p \neq 0$ . Moreover, if  $R_p \neq 0$ , then  $(e_o X_\infty)^\Gamma = 0$  because Iwasawa [13] has shown that  $X_\infty$  has

no finite  $\Lambda$ -submodule other than (0). Therefore, noting that the coefficient of (s-1) in the expansion of  $u^s - u$  is  $u \log u$ , and that

$$|\log u|_p = |u - 1|_p = |w_1(F(\mu_p))|_p,$$

it is now clear that Theorem 1.13 follows from (5), (6), and Lemmas 8 and 9. This completes the proof.

#### REFERENCES

(This only contains papers referred to in these notes).

1. Brumer, A., On the units of algebraic number fields, *Mathematika*, 14 (1967), 121-124.
2. Coates, J., Lichtenbaum, S., On 1-adic zeta functions, *Ann. of Math.*, 98 (1973), 498-550.
3. Coates, J., Sinnott, W., On p-adic L-functions over real quadratic fields, *Inv. Math.*, 25 (1974), 253-279.
4. Coates, J., Sinnott, W., An analogue of Stickelberger's theorem for the higher K-groups, *Inv. Math.*, 24 (1974), 149-161.
5. Coates, J., Sinnott, W., Integrality properties of the values of partial zeta functions, submitted to *Proc. London Math. Soc.*
6. Deligne, P., Ribet, K., Values of abelian L-functions at negative integers, to appear.
7. Greenberg, R., On the Iwasawa invariants of totally real number fields (to appear in *American J. Math.*)

8. Greenberg, R., On  $p$ -adic  $L$ -functions and cyclotomic fields, Nagoya Math. J., 56 (1974), 61-77.
9. Hurwitz, A., Einige Eigenschaften der Dirichlet'schen Funktionen ..., Zeit. für Math. Phys., 27 (1882), 86-101 (Math. Werke I, 72-88).
10. Iwasawa, K., Some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, 16 (1964), 42-82.
11. Iwasawa, K., On the theory of cyclotomic fields, Ann. of Math., 70 (1959), 530-561.
12. Iwasawa, K., On  $p$ -adic  $L$ -functions, Ann. of Math., 89 (1969), 198-205.
13. Iwasawa, K., On  $\mathbb{Z}_\ell$ -extensions of algebraic number fields, Ann. of Math., 98 (1973), 246-326.
14. Iwasawa, K., Lectures on  $p$ -adic  $L$ -functions, Ann. Math. Studies, 74, Princeton, 1972.
15. Kubota, T., Leopoldt, H., Eine  $p$ -adische Theorie der Zetawerte, J. reine angew. Math., 213 (1964), 328-339.
16. Leopoldt, H., Zur Arithmetik in abelschen Zahlkörpern, J. reine angew. Math., 209 (1962), 54-71.
17. Milnor, J., Introduction to algebraic  $K$ -theory, Ann. Math. Studies, 72, Princeton, 1971.
18. Rideout, D., A generalization of Stickelberger's theorem, Ph.D. thesis, McGill University, Montreal (1970).
19. Serre, J.-P., Classes des corps cyclotomiques, Séminaire Bourbaki, Exp. 174 (1958/59).
20. Serre, J.-P., Formes modulaires et fonctions zêta  $p$ -adiques, in Modular functions of one variable III, 191-268, Lecture Notes in Mathematics 350, Springer, 1973.

21. Siegel, C., Bernoullische Polynome und quadratische Zahlkörper, Gött. Nachr., 2, 7-38 (1968).
22. Siegel, C., Über die Fouriersche Koeffizienten von Modulformen, Gött. Nachr., 3, 15-56 (1970).
23. Stickelberger, L., Über eine Verallgemeinerung der Kreistheilung, Math. Ann., 37 (1890), 321-367.

Added in proof. The problem referred to just prior to the beginning of Appendix 1 has recently been solved affirmatively by Ribet. See his paper "A modular construction of unramified extensions of  $\mathbb{Q}(\mu_p)$ ", submitted to Inventiones Math.





H.M. Stark<sup>\*</sup>

## §1. Introduction

In [1] we have formulated a general conjecture on values of Artin L-series at  $s = 1$  (or equivalently values of certain derivatives of L-series at  $s = 0$ ) and proved it for rational characters. Here we will show how to investigate the conjecture numerically in the simplest unproved case. Let  $k$  be a real quadratic field and  $K$  be the ray class field of  $k$  with conductor  $F\bar{p}_\infty$ . The  $\bar{p}_\infty$  means that  $K$  is real while  $K^\beta$  is complex where  $\beta \in G(\bar{\mathbb{Q}}/\mathbb{Q})$  (the Galois group of  $\bar{\mathbb{Q}}/\mathbb{Q}$ ) is non-trivial on  $k$ . We will give examples which show that one can use the numerical values of the derivative of certain L-series at  $s = 0$  to actually determine the field  $K$  (without knowing it beforehand) as well as find a set of  $1/2 [K:k]$  multiplicatively independent units of  $K$  any one of which generates  $K$  over  $\mathbb{Q}$ .

---

<sup>\*</sup> Supported in part by NSF grant MPS 73-08990

For example, let  $k = \mathbb{Q}(\sqrt{5})$ ,  $F = (\frac{11-\sqrt{5}}{2})$ , a principal ideal of norm 29, and  $K$  be the class field of  $k$  corresponding to  $F\bar{p}_\infty$ . Here  $[K:k] = 4$  and  $K/k$  is cyclic. Let  $\psi$  be the ray class character (mod  $F\bar{p}_\infty$ ) such that  $\psi((2)) = i$ . Then numerically (the computer worked with about 16 places), we find

$$\begin{aligned}
 (1) \quad L'(0, \psi) &= (1.656\ 074\ 962\ 913\ 147\dots) \\
 &\quad + i(.205\ 890\ 580\ 538\ 458\ 4\dots) \\
 \log(\varepsilon_+) + i \log(\varepsilon_-) &= (1.656\ 074\ 962\ 913\ 158\dots) \\
 &\quad + i(.205\ 890\ 580\ 538\ 452\ 1\dots)
 \end{aligned}$$

Here (always use the + or the -),

$$(2) \quad \varepsilon_\pm = \frac{(3+2\sqrt{5}) \pm \sqrt{7+2\sqrt{5}} + \sqrt{(20+14\sqrt{5}) \pm (6+4\sqrt{5})\sqrt{7+2\sqrt{5}}}}{4},$$

and either generates  $K$  over  $\mathbb{Q}$ . Naturally we conjecture that

$$L'(0, \psi) = \log(\varepsilon_+) + i \log(\varepsilon_-),$$

but at the moment, all we can prove is

$$(3) \quad |L'(0, \psi)| = |\log(\epsilon_+) + i \log(\epsilon_-)|.$$

In Section 4, we show how to take the numerical value of  $L'(0, \psi)$  in (1) and use it to find  $\epsilon_+$  and  $\epsilon_-$  without even knowing the field  $K$  beforehand. We will also give a second example with  $\mathbb{Q}(\sqrt{229})$  which shows how our conjecture may be used to produce Hilbert class fields of real quadratic fields.

## §2. The numerical evaluation of L-series

Since the L-series we wish to evaluate are at best conditionally convergent at  $s = 1$ , we will say a few words here on how to evaluate them extremely accurately. We are interested in the abelian L-series  $L(s, \psi)$  of conductor  $F\bar{\rho}_\infty$  defined over  $k = \mathbb{Q}(\sqrt{d})$ ,  $d > 0$ . The  $\Gamma$  factor in the functional equation for  $L(s, \psi)$  is usually written as  $\Gamma(\frac{s}{2}) \Gamma(\frac{s+1}{2})$  but for us it is much more convenient to use the duplication formula of the gamma function to write the  $\Gamma$ -factor as  $\Gamma(s)$ . With  $N = dN(F)$ , the functional equation reads

$$(4) \quad \xi(s, \psi) = w \xi(1-s, \bar{\psi})$$

where

$$\xi(s, \psi) = \left( \frac{N}{4\pi^2} \right)^{s/2} \Gamma(s) L(s, \psi)$$

and  $|w| = 1$ .

As we have seen in Serre's lectures [3],  $L(s, \psi)$  therefore corresponds to a modular form on  $\Gamma_0(N)$  (this case was known to Hecke before he even developed the so called Hecke theory). It is convenient for us to normalize things slightly differently. If we write

$$L(s, \psi) = \sum_{n=1}^{\infty} a_n n^{-s}$$

and

$$f(t, \psi) = \sum_{n=1}^{\infty} a_n \exp \left( - \frac{2\pi n}{\sqrt{N}} t \right),$$

then

$$(5) \quad \xi(s, \psi) = \int_0^{\infty} t^{s-1} f(t, \psi) dt.$$

As discovered by Hecke, corresponding to (4) is the transformation formula

$$(6) \quad f(t^{-1}, \psi) = w t f(t, \bar{\psi}) \quad .$$

For any positive real  $u$ , we break the integral in (5) up into two pieces, the first from 0 to  $u$  and the second from  $u$  to  $\infty$ . In the first, we replace  $t$  by  $t^{-1}$  and then use (6), the result is

$$(7) \quad \xi(s, \psi) = w \int_{u^{-1}}^{\infty} t^{-s} f(t, \bar{\psi}) dt + \int_u^{\infty} t^{s-1} f(t, \psi) dt \quad .$$

The value  $u = 1$  leads directly to the functional equation (4); however, larger values of  $u$  will be more useful for us here. We see from (7) that

$$L'(0, \psi) = \xi(0, \psi)$$

$$(8) \quad \begin{aligned} &= w \int_{u^{-1}}^{\infty} f(t, \bar{\psi}) dt + \int_u^{\infty} f(t, \psi) \frac{dt}{t} \\ &= \frac{w\sqrt{N}}{2\pi} \sum_{n=1}^{\infty} \frac{\bar{a}_n}{n} \exp\left(-\frac{2\pi u^{-1}n}{\sqrt{N}}\right) \\ &\quad + \sum_{n=1}^{\infty} a_n \int_u^{\infty} \exp\left(-\frac{2\pi n}{\sqrt{N}} t\right) \frac{dt}{t} \quad . \end{aligned}$$

For values of  $u$  around  $7\sqrt{N}$ , all the integral terms

on the right will be very small and the terms in the first summation with  $n > u^2$  will also be extremely small. What is left gives a few thousand terms which approximate  $L'(0, \psi)$  amazingly accurately. Incidentally, one way this result may be expressed is that  $L(1, \bar{\psi})$  is Abel-summable and extremely rapidly so. Also, by using (8) for several different values of  $u$ , we get an interesting method for numerically integrating  $e^t/t$  over reasonable ranges. This could be useful if examples with much larger values of  $N$  were desired than those that I have considered.

### §3. The form of our conjecture for $K/k$

Let  $G = G(K/k)$  (an Abelian group) so that  $G(K^\beta/k^\beta) = \beta^{-1}G\beta$ . Complex conjugation is an element of  $G(K^\beta/k^\beta)$  and we will denote it by  $\beta^{-1}\tau\beta$  where  $\tau$  in  $G$  is of order 2. It follows easily that for  $\alpha$  in  $K$  and  $\sigma$  in  $G$ ,  $\alpha^{\sigma\beta}$  and  $\alpha^{\tau\sigma\beta} = \alpha^{\sigma\tau\beta}$  are complex conjugate elements of  $K^\beta$ ; we will use this fact several times. Let  $H = G/\{1, \tau\}$ . We let  $F$  be the subfield of  $K$  fixed by  $\tau$  and note that  $G(F/k) = H$ . Further,  $F$  is totally real since  $F^\beta$  is fixed by complex conjugation and so is real. Finally, we let  $n(K)$  denote the degree of  $K$  and  $r(K)$  denote the rank of

the unit group of  $K$ . In this case  $r(K) = |G| + |H| - 1$ .

Lemma 1 (Artin's unit theorem for  $K/k$ ). There are units  $\varepsilon_1$  in  $K$  and  $\varepsilon_2$  in  $F$  such that there is exactly one relation among the  $r(K) + 1$  units,

$$\{\varepsilon_1^\sigma \mid \sigma \in G\} \cup \{\varepsilon_2^\sigma \mid \sigma \in H\}.$$

This relation may be taken to be

$$\prod_{\sigma \in G} (\varepsilon_1 \varepsilon_2)^\sigma = \left( \prod_{\sigma \in G} \varepsilon_1^\sigma \right) \left( \prod_{\sigma \in H} \varepsilon_2^\sigma \right)^2 = \pm 1.$$

Proof. This is just Lemma 6 of [1] specialized to the present situation.

Let  $\chi$  be any (first degree) character of  $G$ . We defined in [1] a matrix  $M(s, \chi) = M(s, \chi, K/k)$  whose determinant has a zero at  $s = 0$  of the same order  $a$  as  $L(s, \chi, K/k)$ . In our case, if  $\chi$  is not the trivial character of  $G$ ,

$$a = 1/2(1 + \chi(1)) + 1/2(1 + \chi(\tau)) = 1 + 1/2(1 + \chi(\tau)).$$



We are interested in those characters  $\psi$  of  $G$  with  $\psi(\tau) = -1$  as these will have the desired value of  $a$  (namely  $a = 1$ ).

The  $\psi$ 's account for half the characters of  $G$ ; the remaining characters of  $G$  will be denoted by  $\chi$ . They have

$\chi(\tau) = 1$  and, as a result, can be thought of as furnishing the characters of  $H$ .

Let

$$(9) \quad B(\sigma) = \begin{cases} \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} & \text{if } \sigma = 1 \\ \begin{pmatrix} 0 & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} & \text{if } \sigma = \tau \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{otherwise} \end{cases}.$$

The matrix  $M(s, \psi)$  of [1] is now given by

$$(10) \quad M(s, \psi) = \sum_{\sigma \in G} \psi(\sigma) \left[ \frac{1}{n(K)} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + B(\sigma) \right. \\ \left. + s \begin{pmatrix} \log | \epsilon_1^\sigma | & \log | \epsilon_1^{\sigma\beta} | \\ \log | \epsilon_2^\sigma | & \log | \epsilon_2^{\sigma\beta} | \end{pmatrix} \right]$$

Since  $\psi$  is non-trivial,  $\sum_{\sigma \in G} \psi(\sigma) = 0$  and this takes care of the first term on the right on (10). Further,  $\psi(\tau) = -1$  and so it follows from (9) that

$$\sum_{\sigma \in G} \psi(\sigma) B(\sigma) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

For the second column of the third matrix we note that for  $i = 1$  or  $2$  and any  $\sigma \in G$ ,

$$\psi(\sigma) \log |\epsilon_i^{\sigma\beta}| + \psi(\sigma\tau) \log |\epsilon_i^{\sigma\tau\beta}| = 0$$

since  $\epsilon_i^{\sigma\tau\beta}$  and  $\epsilon_i^{\sigma\beta}$  are complex conjugates and so have the same absolute value. For the lower left corner of the third matrix, we have for any  $\sigma \in G$ ,

$$\psi(\sigma) \log |\epsilon_2^{\sigma}| + \psi(\tau\sigma) \log |\epsilon_2^{\tau\sigma}| = 0$$

since  $\epsilon_2^{\tau} = \epsilon_2$ . Hence

$$M(s, \psi) = \begin{pmatrix} s \sum_{\sigma \in G} \psi(\sigma) \log |\epsilon_1^{\sigma}| & 0 \\ 0 & 1 \end{pmatrix}$$

and  $\det M(s, \psi)$  has the desired first order zero at  $s = 0$ .

Our conjecture in [1] for this case takes the form

CONJECTURE 1. We have

$$(11) \quad L'(0, \psi, K/k) = c(\psi) \sum_{\sigma \in G} \psi(\sigma) \log |\epsilon_1^\sigma|, \quad ,$$

where  $c(\psi)$  is an algebraic number.

As we only have  $|H|$  characters  $\psi$ , we can't hope to single out each  $|\epsilon_1^\sigma|$  from the L-series values in (11) but we can come close. Let  $\psi_1$  denote one particular character of the  $\psi$ 's (this is not the trivial character of  $G$ ). As  $\chi$  runs through the characters of  $H$ ,  $\chi\psi_1$  runs through the  $\psi$ . We rewrite (11) by grouping the terms  $\sigma$  and  $\tau\sigma$  of  $G$ . This gives our conjecture (11) in the form,

$$(12) \quad L'(0, \chi\psi_1) = c(\chi\psi_1) \sum_{\sigma \in H} \chi(\sigma) \left[ \psi_1(\sigma) \log \left| \left( \frac{\epsilon_1}{\epsilon_1^\tau} \right)^\sigma \right| \right].$$

Here it is important to realize that although  $\psi(\sigma)$  is not defined on  $H$ , the quantities in brackets on the right side are well defined since they are the same for  $\sigma$  and  $\tau\sigma$  in  $G$ .

We are going to investigate the possibility that all the  $c(\chi\psi_1)$  are equal and rational. If we write this common value as  $2r/m$  ( $m$  even allowed) then we are led to

investigate the unit

$$(13) \quad E = \left( \frac{\varepsilon_1}{\varepsilon_1^\tau} \right)^{2r}.$$

Of course the  $E^\sigma$  with  $\sigma \in G$  are not multiplicatively independent since  $E^\tau = 1/E$ . However, this is the only way dependencies arise.

Lemma 2. Let  $\alpha = E + E^{-1}$ . Then  $K = \mathbb{Q}(E^\sigma)$  for any  $\sigma$  in  $G$  and  $F = \mathbb{Q}(\alpha^\sigma)$  for any  $\sigma$  in  $H$ . Further if  $\sigma$  runs through a set of coset representatives of  $\{1, \tau\}$  in  $G$ , then  $E^\sigma$  runs through a set of  $|H|$  independent units of  $K$ .

Proof. The last part of the lemma is a direct corollary of Lemma 1 since the  $\varepsilon_1^\sigma$  are multiplicatively independent for all  $\sigma$  in  $G$ . For the same reason, the  $|G|$  numbers  $E^\sigma$ , with  $\sigma$  running through  $G$ , are distinct. Hence all the conjugates of  $E$  over  $k$  are distinct and therefore  $K = k(E^\sigma)$  for any  $\sigma$  in  $G$ . It follows that  $K^\beta = k(E^{\sigma\beta})$  for any  $\sigma$  in  $G$ . But  $K^\beta$  is complex and so  $E^{\sigma\beta}$  is complex for all  $\sigma$  in  $G$ . Therefore all the conjugates of  $K$  over  $\mathbb{Q}$  are distinct as well and  $K = \mathbb{Q}(E^\sigma)$  for any  $\sigma$

in  $G$ . Finally  $\alpha^\tau = \alpha$  since  $E^\tau = E^{-1}$  and so  $\alpha$  is in  $F$ . But  $E$  is a root of  $x + x^{-1} = \alpha$  and so  $\mathbb{Q}(E)$  is at most a quadratic extension of  $\mathbb{Q}(\alpha)$  and therefore  $F = \mathbb{Q}(\alpha)$ . It follows that  $F = \mathbb{Q}(\alpha^\sigma)$  for any  $\sigma$  in  $H$  as well.

Thanks to the 2 in the exponent in (13),  $E^\sigma > 0$  for all  $\sigma$  in  $G$  and this enables us to drop the absolute value signs in the log terms. Thus, assuming that each  $c(\chi\psi_1) = 2r/m$ , our conjecture becomes,

CONJECTURE 2. There is an integer  $m > 0$  and a unit  $E$  of  $K$  with  $E^\tau = E^{-1}$  such that for each  $\chi$  of  $H$

$$(14) \quad L'(0, \chi\psi_1) = \frac{1}{m} \sum_{\sigma \in H} \chi(\sigma) [\psi_1(\sigma) \log (E^\sigma)] .$$

As  $\sigma$  runs through  $G$ ,  $E^\sigma$  runs through a complete set of conjugates of  $E$  over  $k$ , any one of which generates  $K$  over  $\mathbb{Q}$ . If  $F$  is the fixed field of  $\{1, \tau\}$ , and  $\alpha = E + E^{-1}$ , then the numbers  $\alpha^\sigma$ ,  $\sigma$  in  $H$ , form a complete set of conjugates of  $\alpha$  over  $k$  any one of which generates  $F$  over  $\mathbb{Q}$ .

As far as the integer  $m$  goes, by analogy with what happens with  $k$  complex we should expect that  $m \mid 24|G|$ .

However much more should be true. Indeed, the 10 examples that I have computed as of now all have  $m = 1$  but I would not be surprised to find  $m = 2$  being necessary some day.

#### §4. Two numerical examples.

For any given  $m$ , we may calculate from the numerical values of the  $L'(0, \chi\psi_1)$  numerical values of numbers  $E_m^\sigma$  which, at least for some  $m$ , should be a complete set of conjugate units of  $K$  over  $k$  satisfying Conjecture 2. From these numbers, we calculate numerically the numbers  $\alpha_m^\sigma = E_m^\sigma + E_m^{\tau\sigma} = E_m^\sigma + (E_m^\sigma)^{-1}$ . We then get numerical values of the coefficients of

$$\begin{aligned} g_m(x) &= \prod_{\sigma \in H} (x - \alpha_m^\sigma) \\ &= \sum_{j=0}^{|H|} (-1)^j \theta_{mj} x^{|H|-j}, \end{aligned}$$

where  $\theta_{m0} = 1$ . According to the conjecture, for some  $m$  the numbers  $\theta_{mj}$  will be integers in  $k$ ; they will be furnished to us numerically to about sixteen places (of which the last 3 or 4 are suspect due to round off errors).

We will use these values to produce integers  $\theta_1, \dots, \theta_{|H|}$  in  $k$  which agree numerically with the  $\theta_{mj}$  and then investigate the zeros of the polynomial

$$g(x) = \sum_{j=0}^{|H|} (-1)^j \theta_j x^{|H|-j}$$

where again  $\theta_0 = 1$ . We will let  $\alpha$  denote a zero of  $g(x)$  and  $E$  be a root of  $x + x^{-1} = \alpha$ . If our conjecture is correct,  $E$  should generate  $K$ .

We begin with the example in the introduction. So again,  $k = \mathbb{Q}(\sqrt{5})$ , and  $K$  is the ray class field of  $k$  with conductor  $F\bar{p}_\infty$  where  $F = (\frac{11-\sqrt{5}}{2})$ . The group  $G(K/k)$  is cyclic of order 4. Let  $\psi$  be the ray class character (mod  $F\bar{p}_\infty$ ) with  $\psi((2)) = i$ . We try our conjecture with  $m = 1$ . The value of  $L'(0, \psi)$  in (1) leads us to

$$(15) \quad g_1(x) = x^2 - (7.472 \ 135 \ 954 \ 999 \ 525\dots) x \\ + (11.090 \ 169 \ 943 \ 749 \ 37\dots) \quad .$$

The numbers given here and later are as furnished by the computer with the last three or four digits being dubious.

If our conjecture is true in this case for  $m = 1$  then



the coefficients of  $g_1(x)$  are integers in  $k$ ; however, now we must recognize them. At first glance, this does not seem easy since any real number may be arbitrarily well approximated by integers of  $k$ . Fortunately, we have still more information provided by our conjecture which makes this task simple.

Lemma 3. If  $E$  and  $\alpha$  satisfy conjecture 2, then  $|E^{\sigma\beta}| = 1$  for all  $\sigma$  in  $G$  and  $|\alpha^{\sigma\beta}| < 2$  for all  $\sigma$  in  $H$ .

Proof. According to the conjecture,  $EE^\tau = 1$  and hence  $|E^{\sigma\beta}|^2 = E^{\sigma\beta} E^{\sigma\tau\beta} = (EE^\tau)^{\sigma\beta} = 1$ , which proves the first part of the lemma. Now  $E^{\sigma\beta}$  and  $E^{\tau\sigma\beta}$  are complex conjugate roots of the equation

$$(16) \quad x^2 - \alpha^{\sigma\beta} x + 1 = 0 \quad .$$

Further  $\alpha^{\sigma\beta}$  is real since it generates the real field  $F^\beta$  over  $Q$  and for the roots of (16) to be non-real it is necessary and sufficient that  $|\alpha^{\sigma\beta}| < 2$ , which finishes the lemma.

Remark. It is perhaps surprising that  $|E^{\sigma\beta}| = 1$  but it is less surprising if we remember the specific form of  $E$  that led to conjecture 2. According to (13),  $E^{\sigma\beta} = (\epsilon_1^{\sigma\beta} / \epsilon_1^{\tau\sigma\beta})^{2r}$  is a quotient of complex conjugate numbers and so has absolute value 1.

Returning to our example, we see that our conjecture implies that for  $j = 1$  and  $2$ ,  $|\theta_j^\beta| < 4$ . This restricts the possible values of  $\theta_j$  to a small finite list of integers by the following device: If  $\theta = (a + b\sqrt{d})/2$  is given and  $\theta^\beta = (a - b\sqrt{d})/2$  has absolute value less than  $n$ , then  $b = (\theta - \theta^\beta)/\sqrt{d}$  lies in the range  $[(\theta - n)d^{-\frac{1}{2}}, (\theta + n)d^{-\frac{1}{2}}]$ . To each  $b$ , there is a unique real  $a$  giving  $\theta$  and the correct value of  $b$  makes  $a$  an integer. In this way we find the numbers

$$\theta_1 = 3 + 2\sqrt{5} = 7.472\ 135\ 954\ 999\ 580\dots,$$

$$\theta_2 = \frac{11+5\sqrt{5}}{2} = 11.090\ 169\ 943\ 749\ 47\dots$$

which agree excellently with the numbers in (15).

Let  $\alpha_+$  and  $\alpha_-$  be the larger and smaller roots

respectively of

$$g(x) = x^2 - (3+2\sqrt{5})x + \left(\frac{11+5\sqrt{5}}{2}\right) = 0 \quad .$$

[Note that the discriminant of  $g(x)$  is  $7+2\sqrt{5} = \left(\frac{11-\sqrt{5}}{2}\right) \left(\frac{1+\sqrt{5}}{2}\right)^2$ .] Then the numbers  $\varepsilon_+$  and  $\varepsilon_-$  given in (2) are just the larger roots of  $x + x^{-1} = \alpha_+$  and  $x + x^{-1} = \alpha_-$  respectively. It is easily checked that either  $\varepsilon_+$  or  $\varepsilon_-$  does generate  $K$ . The statement (3) holds because

$$\begin{aligned} |L'(0, \psi)|^2 &= L'(0, \psi) L'(0, \bar{\psi}) \\ &= \frac{1}{2} L''(0, \psi + \bar{\psi}) \end{aligned}$$

where  $\psi + \bar{\psi}$  is a rational character. We gave in [1] an explicit method of calculating L-series with rational characters at  $s = 0$  and it leads in this case to (3).

For our second example, we take  $k = \mathbb{Q}(\sqrt{229})$ , a field of classnumber three, and  $F$  to be the non-principal ideal of norm 3 given by the integral basis,

$$F = \left[3, \frac{5+\sqrt{229}}{2}\right] \quad .$$

The field  $K$  is the ray class field of  $k(\text{mod } \overline{f p}_\infty)$  and is cyclic of degree 6 over  $k$ . On the other hand  $F$  is only of degree 3 over  $k$  and so is the Hilbert class field of  $k$ . Again we try Conjecture 2 with  $m = 1$ . This leads to the cubic polynomial  $g_1(x)$  with coefficients given numerically by

$$\begin{aligned} g_1(x) = & x^3 - (29.132\ 745\ 950\ 421\ 49\dots) x^2 \\ & + (177.796\ 475\ 702\ 529\ 1\dots) x \\ & - (307.327\ 459\ 504\ 215\ 5\dots) \end{aligned}$$

Here we have to find integers  $\theta_1, \theta_2, \theta_3$  in  $\mathbb{Q}(\sqrt{229})$  approximating these values with conjugates having absolute values bounded by 6, 12 and 8 respectively. We take  $\theta_1$  as a particularly nice example. If we set  $\theta_1 = (a+b\sqrt{229})/2$  then  $b$  is seen to lie in the interval  $[(23.132\dots)/\sqrt{229}, (35.132\dots)/\sqrt{229}]$ , an interval of length  $12/\sqrt{229} < 1$ . Thus it was not even guaranteed beforehand that there would be an integer in this interval but in this case  $b = 2$  lies in the interval and we have only one possible value of  $\theta_1$  to examine. This value is

$$14 + \sqrt{229} = 29.132\ 745\ 950\ 421\ 55\dots$$

We naturally take this to be  $\theta_1$ . Similarly, we find the numbers

$$87 + 6\sqrt{229} = 177.796\ 475\ 702\ 529\ 3\dots,$$

and

$$156 + 10\sqrt{229} = 307.327\ 459\ 504\ 215\ 5\dots,$$

which we take to be  $\theta_2$  and  $\theta_3$  respectively. Thus

$$g(x) = x^3 - (14 + \sqrt{229})x^2 + (87 + 6\sqrt{229})x - (156 + 10\sqrt{229}).$$

Our conjecture is that  $g_1(x) = g(x)$ . In any event, it is easily checked that any root of  $g(x) = 0$  does in fact generate  $F$ , the Hilbert class field of  $k$ . Probably the easiest way to do this is to let  $\mu$  be a zero of

$$h(x) = x^3 - 4x - 1,$$

a polynomial of discriminant 229 whose zeros thus generate  $F$ . If

$$\alpha = \frac{1}{\sqrt{229}} \left[ (11+\sqrt{229}) \mu^2 + \left( \frac{49+5\sqrt{229}}{2} \right) \mu + (47+2\sqrt{229}) \right]$$

then  $\alpha$  is a zero of  $g(x)$ . Of course  $g(x)$  has messier coefficients than  $h(x)$ , but it must be remembered that  $g(x)$  should provide us with units in a bigger class field of  $k$ . In fact if  $E$  is a root of  $x+x^{-1} = \alpha$ , then  $K = \mathbb{Q}(E)$ , as it should.

These two examples make Conjecture 2 appear unassailable but I have already calculated several other examples and will do more shortly. I expect to report on these in fuller detail in [2]. Further, one can formulate a conjecture analogous to Conjecture 2 for all other totally real fields and there also the conjecture appears to contain enough information to enable one to calculate class fields of totally real fields without knowing them beforehand. This too will be reported on in [2] and, if my computer budget can stand it (which is not clear at this point), one or two numerical examples will be provided for cubic fields.

## REFERENCES

1. H.M. Stark, L-functions at  $s = 1$ . II. Artin L-functions with rational characters, *Advances in Math.*, 17 (1975), 60-92.
2. \_\_\_\_\_, L-functions at  $s = 1$ , part III, to be published.
3. J.P. Serre, Modular forms of weight one, *Durham Symposium*.





# On Conductors and Discriminants

A.M. Odlyzko

## §1. Introduction

Let  $K$  be a normal algebraic number field with Galois group  $G = G(K/Q)$ , and suppose that  $\chi$  is a character of  $G$  and  $F(\chi)$  the conductor of  $\chi$ . It follows easily from the definition of the conductor that  $F(\chi) > 1$  if  $\chi$  is not a multiple of the identity character [2, pp. 165-194]. On the other hand, it seems very hard to obtain good lower bounds for  $F(\chi)$ , especially if  $\chi(1)$  is large. The usual geometry of numbers methods used for dealing with discriminants do not apply to the case of conductors, even though the two are related by the famous "Führerdiskriminantenproduktformel."

Recently this author [10-12] has used a new analytic method to obtain estimates for discriminants which are better than the previous geometry of numbers bounds. A crucial role in this method was played by the functional

equation of the Dedekind zeta function. Since Artin L-functions also possess functional equations, J.-P. Serre and H.M. Stark have asked whether it might not be possible to use a similar method to obtain bounds for conductors. The purpose of this note is to show that this is indeed possible, provided we restrict ourselves to characters for which Artin's conjecture holds.

Let us define  $a = a(\chi)$ ,  $b = b(\chi)$  by

$$a = \frac{1}{2} (\chi(1) + \chi(g_0)), \quad b = \frac{1}{2} (\chi(1) - \chi(g_0)), \quad (1.1)$$

where  $g_0$  is the element of  $G(K/Q)$  corresponding to complex conjugation if  $K$  is not real, and  $g_0 = 1$  if  $K$  is real.

Also, we let

$$G(a, b, s) = -a \frac{\Gamma'}{\Gamma} \left( \frac{s}{2} \right) - b \frac{\Gamma'}{\Gamma} \left( \frac{s+1}{2} \right). \quad (1.2)$$

$G'(a, b, s)$  will denote the derivative of  $G(a, b, s)$  with respect to  $s$ . We now state our main result, which will be proved in Section 2.

Theorem 1. Suppose that  $\operatorname{Re} \chi(g) \geq 0$  for all

$g \in G(K/Q)$  and that for some integer  $r$ ,  $(s-1)^r L(s, \chi)$  is entire. Then

$$F(\chi) \geq (60.1)^{a-b} (22.2)^{2b} e^{-254r} \quad , \quad (1.3)$$

$$F(\chi) \geq (58.6)^{a-b} (21.8)^{2b} e^{-70r} \quad , \quad (1.4)$$

and if  $\sigma > 1$ ,  $\tilde{\sigma} > 1$  are real numbers satisfying

$$\tilde{\sigma} \geq \frac{5 + \sqrt{12\sigma^2 - 5}}{6} \quad (1.5)$$

and

$$\tilde{\sigma} \geq 1 + \alpha\sigma \quad , \quad (1.6)$$

where  $\alpha = 0.28108\dots$ , then

$$\begin{aligned} \log F(\chi) &\geq \chi(1) \log \pi + G(a, b, \sigma) - \left(\sigma - \frac{1}{2}\right) G'(a, b, \tilde{\sigma}) \\ &+ r \left\{ -\frac{2}{\sigma} - \frac{2}{\sigma-1} - \frac{2\sigma-1}{\tilde{\sigma}^2} - \frac{2\sigma-1}{(\tilde{\sigma}-1)^2} \right\} \quad . \quad (1.7) \end{aligned}$$

If, in addition to being entire,  $(s-1)^r L(s, \chi)$  also satisfies the Generalized Riemann Hypothesis (GRH), then

we have

$$F(x) \geq (188.3)^{a-b} (41.6)^{2b} e^{-3.7 \times 10^8 r} \quad (1.8)$$

and (1.7) holds whenever  $\sigma > 1$ ,  $\tilde{\sigma} > 1$  satisfy

$$\tilde{\sigma} \geq \frac{1}{2} + \frac{\sigma - \frac{1}{2}}{\sqrt{3}} \quad (1.9)$$

We will now derive several corollaries from Theorem 1, the first of which will give the discriminant bounds of [11] and [12]. (We should note, however, that the argument is somewhat circular, as the proof of Theorem 1 is essentially a corollary to the proofs of [11] and [12].)

Corollary 1. Let  $k$  be any (i.e., not necessarily normal) algebraic number field,  $D$  the absolute value of the discriminant of  $k$ , and  $r_1$  and  $2r_2$  the numbers of real and complex conjugate fields, respectively. Then

$$D \geq (60.1)^{r_1} (22.2)^{2r_2} e^{-254}, \quad (1.10)$$

$$D \geq (58.6)^{r_1} (21.8)^{2r_2} e^{-70}, \quad (1.11)$$

and

$$\begin{aligned} \log D &\geq (r_1 + 2r_2) \log \pi + G(r_1 + r_2, r_2, \sigma) \\ &\quad - \left(\sigma - \frac{1}{2}\right) G(r_1 + r_2, r_2, \tilde{\sigma}) \\ &\quad - \frac{2}{\sigma-1} - \frac{2}{\sigma} - \left(\sigma - \frac{1}{2}\right) \left\{ \frac{2}{(\tilde{\sigma}-1)^2} + \frac{2}{\tilde{\sigma}^2} \right\} \end{aligned} \quad (1.12)$$

for any  $\sigma > 1$ ,  $\tilde{\sigma} > 1$  which satisfy (1.5) and (1.6). If the zeta function of  $k$  satisfies the GRH, then

$$D \geq (188.3)^{r_1} (41.6)^{2r_2} e^{-3.7 \times 10^8} \quad (1.13)$$

and (1.12) holds for any  $\sigma > 1$ ,  $\tilde{\sigma} > 1$  which satisfy (1.9).

Proof of Corollary 1. Let  $K$  be a normal number field containing  $k$ , and let  $G(K/Q)$  be the Galois group of  $K$ . Let  $H$  be the subgroup of  $G(K/Q)$  which fixes  $k$ , and  $\phi$  the identity character of  $H$ . If  $\phi^*$  is the character of  $G(K/Q)$  induced by  $\phi$ , then  $\phi^*(g) \geq 0$  for all  $g \in G(K/Q)$ ,  $F(\phi^*) = D$ , and since

$$L(s, \phi^*) = L(s, \phi, K/k) = \zeta_k(s),$$

$(s-1)L(s, \phi^*)$  is entire. Corollary 1 now follows immediately from Theorem 1.

In general, if  $\chi$  is a character of  $G(K/Q)$ , then its real part does take on negative values. In those cases we can consider the character  $\chi + m\chi_0$ , where  $\chi_0$  is the identity character of  $G(K/Q)$  and  $m$  is a positive integer (and, in fact, by considering  $n\chi + h\chi_0$  for positive integers  $n$  and  $h$ , we could in effect consider  $\chi + m\chi_0$  for any positive real number  $m$ ). If  $m$  is large enough, then  $\operatorname{Re}(\chi + m\chi_0) \geq 0$ , and Theorem 1 can be applied to estimate  $F(\chi + m\chi_0) = F(\chi)$ .

Corollary 2. Suppose that  $\chi$  is a character of  $G(K/Q)$  such that  $(s-1)^{\chi(1)} \zeta_Q^{\chi(1)}(s)L(s, \chi)$  is entire. Then

$$F(\chi) > (3.70)^a (2.38)^b, \quad (1.14)$$

$$F(\chi) > (3.85)^a (2.27)^b, \quad (1.15)$$

and if  $\zeta_Q^{\chi(1)}(s)L(s, \chi)$  satisfies also the GRH, then even



$$F(\chi) > (3.93)^a (2.50)^b, \quad (1.16)$$

$$F(\chi) > (4.10)^a (2.39)^b. \quad (1.17)$$

Proof of Corollary 2. Since  $\operatorname{Re} \chi(g) \geq -\chi(1)$  for all  $g \in G(K/Q)$ , we have  $\operatorname{Re}(\chi + \chi(1)\chi_0) \geq 0$ . Also  $(s-1)^{\chi(1)} L(s, \chi + \chi(1)\chi_0)$  is entire by the hypothesis of the corollary. Hence we can apply Theorem 1. Putting  $\sigma = 7.8$ ,  $\tilde{\sigma} = 5.32\dots$ , in (1.7) gives (1.14);  $\sigma = 6.295$ ,  $\tilde{\sigma} = 4.44\dots$  gives (1.15);  $\sigma = 9.18$ ,  $\tilde{\sigma} = 5.51\dots$  gives (1.16); and finally,  $\sigma = 7.655$ ,  $\tilde{\sigma} = 4.63\dots$  gives (1.17).

For one-dimensional characters the bounds of Corollary 2 (especially those implied by the GRH) are not far from best possible, since quadratic fields yield an example of a character  $\chi$  with  $\chi(1) = 1$ ,  $a = 1$ ,  $b = 0$ , and  $F(\chi) = 5$ , as well as of a character  $\chi$  with  $\chi(1) = 1$ ,  $a = 0$ ,  $b = 1$ , and  $F(\chi) = 3$ . (The corresponding  $L(s, \chi)$  are entire, since the  $\chi$  are one-dimensional.) However, if  $\chi(1)$  is large, one can obtain significantly better estimates (but under different assumptions) as will be shown below. At the end of Section 2 we will also show how one can obtain a

similar but slightly better estimate than the one of Corollary 2. We should also mention that for many characters  $\chi$ ,  $\operatorname{Re}(\chi + m\chi_0) \geq 0$  for  $m$  much smaller than  $\chi(1)$ , which leads to much better results.

Since for any character  $\chi$ , the character  $\chi\bar{\chi}$  is non-negative, Theorem 1 gives a lower bound for  $F(\chi\bar{\chi})$ . This bound, in turn, can be used to obtain a lower bound for  $F(\chi)$ , as is shown by the following lemma, which will be proved in Section 2.

Lemma 1.  $F(\chi\bar{\chi})$  divides  $F(\chi)^{2(\chi(1)-1)}$ .

Lemma 1 implies that

$$F(\chi\bar{\chi}) \leq F(\chi)^{2(\chi(1)-1)},$$

and so any lower bound for  $F(\chi\bar{\chi})$  gives a lower bound for  $F(\chi)$ . Suppose, for example, that  $\chi$  is an irreducible character such that  $L(s, \chi\bar{\chi})$  is analytic for  $s \neq 1$ . Then  $(s-1)L(s, \chi\bar{\chi})$  is entire, and so Theorem 1 (applied with  $\chi$  replaced by  $\chi\bar{\chi}$ ) and Lemma 1 yield the asymptotic bound

$$F(\chi) \geq (7.75) \frac{\chi(g_0)^2}{\chi(1)} \quad (4.71) \quad \frac{\chi(1)^2 - \chi(g_0)^2}{\chi(1)} + O(1)$$

as  $\chi(1) \rightarrow \infty$ ,

and if the GRH holds for  $L(s, \chi\bar{\chi})$ , then even

$$F(\chi) \geq (13.72) \frac{\chi(g_0)^2}{\chi(1)} \quad (6.44) \quad \frac{\chi(1)^2 - \chi(g_0)^2}{\chi(1)} + O(1)$$

as  $\chi(1) \rightarrow \infty$ .

Of course, one can also obtain non-asymptotic bounds for  $F(\chi)$  this way, and some of them are given in Table 4.

Before concluding this section, we should say a few words about applying the estimate (1.7). In order to obtain the best results for given  $a$ ,  $b$ , and  $r$ , one should define  $\tilde{\sigma}$  as a function of  $\sigma$  to be the smallest number satisfying (1.5) and (1.6) (or (1.9), if the GRH is being assumed) and then search for the best value of  $\sigma$ . Some indication of the appropriate value can be obtained from our tables, which are described in Section 3. We should also mention that it is possible to obtain significantly

better results if, say,  $-(L'/L)(s)$  is large for some  $s > 1$ . The argument here is analogous to that of [11] and [12].

We conclude this section with a new application of bounds for discriminants. Let  $\zeta$  be a primitive  $m$ -th root of unity, and let  $K_m = \mathbb{Q}(\zeta + \zeta^{-1})$  be the maximal real subfield of the cyclotomic field  $\mathbb{Q}(\zeta)$ . If  $h_0(m)$  denotes the class number of  $K_m$ , then  $h_0(m)$  is the second factor of the class number of  $\mathbb{Q}(\zeta)$ . It often equals 1 [3], but it is greater than 1 in some cases [1]. One still unsolved problem concerns  $h_0(2^k)$ . Bauer [3] has shown that  $h_0(64) = 1$ , thus disproving a conjecture of Weber [15; vol. 2, pp. 808]. We will now give a new proof of this result. Let  $D$  be the discriminant of  $K_{64}$ , and let  $h_0 = h_0(64)$ . Then an easy calculation shows that

$$D = 2^{79}$$

Next let  $H$  be the Hilbert class field of  $K_{64}$ . Then  $H$  is a totally real number field of degree  $h_0$   $[K_{64}:\mathbb{Q}] = 16 h_0$  and discriminant

$$D^h_0 = 2^{79 \cdot h_0} = (30.643\dots)^{16h_0}.$$

But Table 1 shows that this is impossible if  $16.h_0 \geq 96$ .

Hence  $h_0 \leq 5$ , and so by [4] one must have  $h_0 = 1$ .

Our unconditional bounds are too weak to apply to  $K_{2^k}$  for  $k \geq 7$ . However, if we assume the GRH then a similar argument will yield  $h_0(128) = 1$  (setting  $\sigma = 1.62$ ,  $\tilde{\sigma} = \frac{1}{2} + (\sigma - \frac{1}{2})/\sqrt{3}$  in (1.12) leads to the conclusion that  $h_0(128) \leq 23$ , which together with [4] proves the result), and that  $h_0(256) \leq 14,600,000$  (here we use (1.13)). We should also mention that John Masley has used these methods together with his own results to prove  $h_0(m) = 1$  for some additional values of  $m$ .

## §2. Proofs

At the beginning of this section we consider a slightly more general situation than before. We let  $k$  be any number field and  $K$  a normal extension of  $k$  with Galois group  $G(K/k)$ . If  $\chi$  is a character of  $G(K/k)$ , then the Artin L-function  $L(s, \chi)$  is defined by

$$\log L(s, \chi) = \sum_P \sum_{m=1}^{\infty} \frac{1}{m} \chi_k(P^m) (NP)^{-ms} \quad \text{for } \operatorname{Re}(s) > 1,$$

(2.1)

where  $P$  runs through all the prime ideals of  $k$ ,  $N$  denotes

the norm from  $k$  to  $Q$ , and

$$\chi_k(P^m) = \frac{1}{e} \sum_{\alpha \in I} \chi(\tau^m \alpha),$$

where  $I$  is the inertia group of any one of the prime ideal factors of  $P$  in  $K$ ,  $e = |I|$ , and  $\tau$  is one of the Frobenius automorphisms corresponding to  $P$ . One obvious result we will use later is that

$$|\chi_k(P^m)| \leq \chi(1). \quad (2.2)$$

Let us also recall that for real  $\chi$  there exist positive integers  $a = a(\chi)$  and  $b = b(\chi)$  such that if

$$\xi(s, \chi) = \left( \frac{d^{\chi(1)} N(F(\chi))}{\pi^{\chi(1)} [k:Q]} \right)^{s/2} \Gamma\left(\frac{s}{2}\right)^a \Gamma\left(\frac{s+1}{2}\right)^b L(s, \chi), \quad (2.3)$$

where  $d$  is the absolute value of the discriminant of  $k$ , then  $\xi(s, \chi)$  satisfies the functional equation

$$\xi(1-s, \bar{\chi}) = W(\chi) \xi(s, \chi), \quad (2.4)$$

where  $W(\chi)$  is a certain constant (of absolute value 1, but

we will not need that fact). The facts we do need to know about  $a(\chi)$  and  $b(\chi)$  is that  $a(\chi) = a(\bar{\chi})$ ,  $b(\chi) = b(\bar{\chi})$ , and that if  $k = Q$ , then they are defined by (1.1).

Next we will derive a relation between  $F(\chi)$  and the zeroes of  $L(s, \chi)$  which generalizes the identities relating the discriminant to the zeroes of the corresponding zeta function [10; Lemma 1], [14; Lemma 1]. Most of the steps in the proof below are standard and are only briefly outlined. The crucial result, the identity (2.8) dates back at least to Landau [5, vol. 1; pp. 313-317], [6-7], and can be proved in several different ways.

Lemma 2. Suppose that  $(s-1)^r L(s, \chi)$  is entire for some non-negative integer  $r$ , and suppose that  $r$  is the smallest integer with this property. Then

$$\log N(F(\chi)) = \chi(1) [k:Q] \log \pi - \chi(1) \log d + G(a, b, s)$$

$$- \frac{L'}{L}(s, \chi) - \frac{L'}{L}(s, \bar{\chi}) + \sum_{\rho} \left\{ \frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}} \right\} - \frac{2r}{s-1} - \frac{2r}{s}, \quad (2.5)$$

identically in the complex variable  $s$ , where  $\rho = \beta + i\gamma$  runs through the nontrivial zeros of  $L(s, \chi)$  (i.e., those



zeroes  $\rho$  for which  $0 < \beta < 1$ ), and  $G(a,b,s)$  is defined by (1.2).

Proof. Since  $(s-1)^r L(s,\chi)$  is entire, so is  $(s-1)^r L(s,\bar{\chi})$ , and so if we set

$$f(s) = [s(s-1)]^{2r} \xi(s,\chi) \xi(s,\bar{\chi}), \quad (2.6)$$

then  $f(s)$  is an entire function and satisfies

$$f(1-s) = W(\chi) W(\bar{\chi}) f(s) . \quad (2.7)$$

Furthermore,  $f(s)$  is real for real  $s$ , so that if  $z$  is a zero of  $f(s)$ , then so are  $\bar{z}$ ,  $1-\bar{z}$ , and  $1-z$ . Also, since the zeros of  $f(s)$  are precisely the nontrivial zeroes of  $L(s,\chi) L(s,\bar{\chi})$ , they all lie in the critical strip.

Using the fact that  $f(s)$  is entire one can easily show that it is in fact of order one, so that by the Hadamard factorization theorem

$$f(s) = e^{A+Bs} \prod_{\rho} \left\{ \left(1 - \frac{s}{\rho}\right) \left(1 - \frac{s}{\bar{\rho}}\right) e^{s/\rho + s/\bar{\rho}} \right\}$$

for some constants  $A$  and  $B$ , where  $\rho$  runs through the nontrivial zeros of  $L(s, \chi)$ . Hence

$$\frac{f'}{f}(s) = B + \sum_{\rho} \left\{ \frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}} + \frac{1}{\rho} + \frac{1}{\bar{\rho}} \right\}$$

But by (2.7),

$$\frac{f'}{f}(s) = -\frac{f'}{f}(1-s),$$

which implies

$$B + \sum_{\rho} \left\{ \frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}} + \frac{1}{\rho} + \frac{1}{\bar{\rho}} \right\} = -B - \sum \left\{ \frac{1}{1-s-\bar{\rho}} + \frac{1}{1-s-\rho} + \frac{1}{\rho} + \frac{1}{\bar{\rho}} \right\}.$$

Since  $1-\bar{\rho}$  is a nontrivial zero of  $L(s, \chi)$  whenever  $\rho$  is, we discover that

$$B = \sum_{\rho} \left\{ \frac{1}{\rho} + \frac{1}{\bar{\rho}} \right\}, \quad (2.8)$$

$$\frac{f'}{f}(s) = \sum_{\rho} \left\{ \frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}} \right\}$$

which together with (2.3), (2.6), and the fact that

$F(\chi) = F(\bar{\chi})$  completes the proof of the lemma.

Although we have proved Lemma 2 for characters of general extensions  $K/k$ , we will actually use it only for  $k = \mathbb{Q}$ . The reason for this generality is that Eq. (2.5) is useful in obtaining results about zeros of L-functions.

Proof of Theorem 1. Let us now consider (2.5) for  $k = \mathbb{Q}$  and  $s$  real. We then obtain

$$\begin{aligned} \log F(\chi) &= \chi(1)\log \pi + G(a,b,s) - 2 \operatorname{Re} \frac{L'}{L}(s,\chi) \\ &\quad + 2 \sum_{\rho} \operatorname{Re} \frac{1}{s-\rho} - \frac{2r}{s-1} - \frac{2r}{s}, \end{aligned} \tag{2.9}$$

where  $a$  and  $b$  are defined by (1.1). The most important property of (2.9) as far as further work is concerned is that for  $s > 1$  and any nontrivial zero  $\rho = \beta + i\gamma$

$$\operatorname{Re} \frac{1}{s-\rho} = \frac{s-\beta}{|s-\rho|^2} > 0,$$

and so the sum over the zeros in (2.9) is positive. Our aim will be to show that it is in fact quite large.

The basic idea of our proof is to use derivatives of (2.9) to obtain information about the sum of  $\operatorname{Re}(s-\rho)^{-1}$ . Differentiating (3.9) once and setting  $s = \tilde{\sigma}$  yields

$$2 \sum_{\rho} \operatorname{Re} \frac{-1}{(\tilde{\sigma}-\rho)^2} = -G'(a, b, \tilde{\sigma}) \quad (2.10)$$

$$+ 2 \operatorname{Re} \left( \frac{L'}{L} \right)'(\tilde{\sigma}, \chi) - \frac{2r}{(\tilde{\sigma}-1)^2} - \frac{2r}{\tilde{\sigma}^2} .$$

Our goal will be to show that

$$\sum_{\rho} \operatorname{Re} \frac{1}{\sigma-\rho} \geq \left(\sigma - \frac{1}{2}\right) \sum_{\rho} \operatorname{Re} \frac{-1}{(\tilde{\sigma}-\rho)^2} \quad (2.11)$$

for as wide a range of  $\sigma$  and  $\tilde{\sigma}$  as possible. Since  $\operatorname{Re} \chi \geq 0$ , we have

$$- \operatorname{Re} \frac{L'}{L}(\sigma, \chi) \geq 0 ,$$

$$\operatorname{Re} \left( \frac{L'}{L} \right)'(\tilde{\sigma}, \chi) \geq 0 ,$$

and so (2.11) implies (1.7). Thus the critical point is the proof of (2.11). Let us first assume that  $L(s, \chi)$

satisfies the GRH, so that all the nontrivial zeroes  $\rho$  are of the form  $\rho = \frac{1}{2} + i\gamma$ . Hence to prove (2.11) we have to show that

$$\sum_{\rho} \frac{\sigma - \frac{1}{2}}{(\sigma - \frac{1}{2})^2 + \gamma^2} \geq (\sigma - \frac{1}{2}) \sum_{\rho} \frac{\gamma^2 - (\tilde{\sigma} - \frac{1}{2})^2}{((\tilde{\sigma} - \frac{1}{2})^2 + \gamma^2)^2} \quad (2.12)$$

However, a simple cross-multiplication shows that

$$\frac{1}{(\sigma - \frac{1}{2})^2 + \gamma^2} \geq \frac{\gamma^2 - (\tilde{\sigma} - \frac{1}{2})^2}{((\tilde{\sigma} - \frac{1}{2})^2 + \gamma^2)^2}$$

holds for all real  $\gamma$  if (1.9) is satisfied, and this proves (2.12) (and hence also (1.7)) subject to (1.9) and the GRH. To prove (2.11) without the assumption of the GRH, we note that if  $\rho$  is a nontrivial zero, then it is  $1 - \bar{\rho}$ . Hence (2.11) is equivalent to

$$\sum_{\rho} \operatorname{Re} \left\{ \frac{1}{\sigma - \rho} + \frac{1}{\sigma - 1 + \bar{\rho}} \right\} \geq (\sigma - \frac{1}{2}) \sum_{\rho} \operatorname{Re} \left\{ \frac{1}{(\sigma - \rho)^2} + \frac{1}{(\tilde{\sigma} - 1 + \bar{\rho})^2} \right\},$$

which will certainly hold if

$$\operatorname{Re} \left\{ \frac{1}{\sigma - \rho} + \frac{1}{\sigma - 1 + \bar{\rho}} \right\} \geq (\sigma - \frac{1}{2}) \operatorname{Re} \left\{ \frac{-1}{(\tilde{\sigma} - \rho)^2} + \frac{-1}{(\tilde{\sigma} - 1 + \bar{\rho})^2} \right\}$$

holds for all  $\rho$ . This, however, can also easily be shown to hold, provided (1.5) and (1.6) are satisfied. Details are available in [11; Lemma 1]. This process gives (1.7) subject only to (1.5) and (1.6).

To obtain (1.3), (1.4), and (1.8) we apply the proofs of [12], which show that

$$\sum_{\rho} \operatorname{Re} \frac{1}{\sigma - \rho} > \sum_j a_j \sum_{\rho} \operatorname{Re} \frac{-1}{(\sigma_j - \rho)^{k_j}} \quad (2.13)$$

for appropriate choices of  $\sigma_j > 1$ ,  $a_j > 0$ , and  $k_j \geq 2$ , where the only constraints on the  $\rho$ 's were that they should lie in the critical strip (on the critical line in the GRH case) and that if  $z$  is one of them, then so is  $1 - \bar{z}$ . But by differentiating (2.9) we find that for  $u > 1$ ,  $k \geq 2$ ,

$$(k-1)! \sum \operatorname{Re} \frac{-1}{(u-\rho)^k} \geq \frac{1}{2} |G^{(k-1)}(a, b, u)|$$

$$- \frac{r(k-1)!}{(u-1)^k} - \frac{r(k-1)!}{u^k},$$

and so any result of the form (2.13) leads to an improved estimate for  $F(\chi)$ . In particular, if we carry out the computations for the choices in [12], we obtain (1.3),

(1.4), and (1.8). This finishes the proof of Theorem 1.

Proof of Lemma 1. In view of the definition of the conductors [2; p. 188] it suffices to show that for every subgroup  $H$  of  $G(K/Q)$

$$|H| \chi(1)^2 - \chi \bar{\chi}(H) \leq 2 (\chi(1) - 1) (|H| \chi(1) - \chi(H)),$$

where for any function  $f$  on  $G(K/Q)$ ,  $f(H) = \sum_{h \in H} f(h)$ .

We suppose that

$$\chi|_H = r \cdot \phi_0 + \sum_{i \geq 1} r_i \cdot \phi_i, \quad (1.18)$$

where  $\phi_0$  is the identity character of  $H$ , and the  $\phi_i$  are the nontrivial irreducible characters of  $H$ . Then

$$\chi(u) = r|H|, \quad \chi \bar{\chi}(H) = \left\{ r^2 + \sum_{i \geq 1} r_i^2 \right\} |H|,$$

and we have to prove that

$$\chi(1)^2 - r^2 - \sum_{i \geq 1} r_i^2 \leq 2(\chi(1) - 1) (\chi(1) - r),$$



i.e., that

$$(\chi(1) - r) (\chi(1) - r - 2) \geq - \sum_{i \geq 1} r_i^2 . \quad (1.19)$$

But by (1.18),

$$\chi(1) = r + \sum_{i \geq 1} r_i \phi_i(1) ,$$

and so we have to prove that

$$\left( \sum_{i \geq 1} r_i \phi_i(1) \right) \left( \sum_{i \geq 1} r_i \phi_i(1) - 2 \right) \geq - \sum_{i \geq 1} r_i^2 .$$

But the left side above is negative only when  $r_j = \phi_j(1) = 1$  for exactly one value of  $j$ , all other  $r_j$  being equal to zero, in which case both sides equal  $-1$ . In all other cases the left side is non-negative, while the right side is non-positive and so this inequality holds always, which proves the lemma.

It is possible to obtain results similar to those of Corollary 2 by proceeding slightly differently than in the proof of Theorem 1. For example, if we don't assume

$\operatorname{Re} \chi \geq 0$ , then we have for  $\sigma > 1$ ,  $\tilde{\sigma} > 1$

$$- \operatorname{Re} \frac{L'}{L}(\sigma, \chi) \geq \chi(1) \frac{\zeta'}{\zeta}(\sigma)$$

$$\operatorname{Re} \left( \frac{L'}{L} \right)'(\tilde{\sigma}, \chi) \geq \chi(1) \left[ - \left( \frac{\zeta'}{\zeta} \right)'(\tilde{\sigma}) \right] .$$

Combining this with (2.9)-(2.11) (which hold irrespective of what values  $\chi$  takes, subject only to (1.5) and (1.6) (or (1.9) in the GRH case)) leads to slightly better estimates than those of Corollary 2, but this time under the assumption that  $L(s, \chi)$  rather than  $L(s, \chi + \chi(1)\chi_0)$  satisfies Artin's conjecture.

### §3. Description of tables

Table 1 evaluates the bounds of Corollary 1 for totally real and totally complex fields of some relatively low degrees, with only the best bound being shown. A numerical value for  $\sigma$  means that the corresponding bound was obtained by evaluating (1.7) with that value of  $\sigma$  and with  $\tilde{\sigma}$  chosen to satisfy (1.5) with equality in the case of the unconditional bound and to satisfy (1.9) with equality in the case of the GRH bound. The notation

"Ineq. (1.11)", on the other hand, means that the corresponding bound follows from (1.11). We should note that because of the form our bounds take a bound for  $D^{1/n}$  for a totally complex field of degree  $n = n_0$  is a bound for  $D^{1/n}$  for all fields of degrees  $n \geq n_0$ , and a bound for a totally real field of degree  $n = n_0$  is a bound for all totally real fields of degrees  $n \geq n_0$ . The bounds in Table 1, as well as in the other tables, have all been rounded down.

In Table 2, the second column presents the minimal value of  $D^{1/n}$  that any totally real field of degree  $n$  can have [8; p. 81], [13]. The remaining columns show the bounds of Corollary 1 for these values of  $n$  and are constructed in the same way as Table 1.

Table 3 similarly compares our bounds for discriminants of totally complex fields with some known low values. In this case, however, the values of  $D^{1/n}$  in the second column are not known to be optimal except for  $n = 4$  [8; p. 81]. The values of  $D^{1/n}$  for  $n = 8, 14, 20$ , and  $28$  come from the Hilbert class fields of  $Q(\sqrt{-d})$  with  $d = 39, 71, 119$ , and  $215$ , respectively. The  $n = 48$  value comes from the field associated with the

TABLE 1  
Lower Bounds for Discriminants

Unconditional Bound				GRH Bound			
k totally real		k totally complex		k totally real		k totally complex	
n	$\sigma$	$D^{1/n}$	$\sigma$	$D^{1/n}$	$\sigma$	$D^{1/n}$	$\sigma$
6	2.435	6.35	3.1	3.89	3.695	6.82	4.425
8	2.055	8.27	2.57	4.77	3.275	8.98	3.865
10	1.845	10.00	2.26	5.53	3.025	10.93	3.525
12	1.705	11.54	2.055	6.17	2.855	12.70	3.295
14	1.61	12.94	1.91	6.74	2.73	14.30	3.125
16	1.54	14.20	1.805	7.25	2.635	15.76	2.995
18	1.485	15.35	1.725	7.70	2.555	17.11	2.895
20	1.445	16.40	1.655	8.11	2.495	18.35	2.81
24	1.38	18.26	1.56	8.82	2.395	20.57	2.675
28	1.335	19.86	1.49	9.41	2.32	22.51	2.58
32	1.3	21.24	1.44	9.93	2.26	24.24	2.5
36	1.275	22.47	1.40	10.38	2.215	25.78	2.435
40	1.255	23.55	1.37	10.77	2.175	27.17	2.385
44	1.24	24.53	1.34	11.13	2.14	28.45	2.34
48	1.225	25.41	1.32	11.44	2.11	29.61	2.3
52	1.21	26.21	1.30	11.73	2.085	30.69	2.27
56	1.2	26.94	1.285	11.99	2.06	31.69	2.24
60	1.19	27.61	1.27	12.23	2.04	32.62	2.21

64	1.185	28.23	1.26	12.45	2.025	33.49	2.19	13.67
68	1.175	28.80	1.245	12.65	2.005	34.30	2.165	13.92
72	1.17	29.34	1.235	12.84	1.99	35.07	2.145	14.15
76	1.165	29.84	1.23	13.01	1.975	35.80	2.13	14.37
80	1.16	30.30	1.22	13.18	1.965	36.48	2.11	14.57
84	1.155	30.74	1.215	13.33	1.95	37.13	2.095	14.76
88	1.15	31.15	1.205	13.47	1.94	37.75	2.08	14.94
92	1.145	31.54	1.2	13.61	1.93	38.34	2.07	15.12
96	1.14	31.91	1.195	13.74	1.92	38.91	2.055	15.28
100	1.135	32.26	1.19	13.86	1.91	39.45	2.045	15.44
110	1.13	33.05	1.175	14.13	1.89	40.70	2.02	15.79
120	1.12	33.75	1.165	14.38	1.87	41.83	1.995	16.12
130	1.115	34.26	1.16	14.59	1.855	42.86	1.975	16.41
140	Ineq.(1.11)	35.54	1.15	14.79	1.84	43.81	1.955	16.67
150	"	36.74	1.145	14.96	1.83	44.69	1.94	16.92
160	"	37.83	1.14	15.12	1.815	45.50	1.925	17.14
170	"	38.82	1.135	15.27	1.805	46.26	1.91	17.35
180	"	39.71	1.13	15.40	1.795	46.96	1.9	17.54
190	"	40.54	1.125	15.53	1.79	47.63	1.89	17.72
200	"	41.29	1.12	15.64	1.78	48.25	1.875	17.89
220	"	42.62	Ineq.(1.11)	15.85	1.765	49.40	1.86	18.20
240	"	43.77	"	16.28	1.75	50.43	1.84	18.48
260	"	44.76	"	16.65	1.74	51.37	1.825	18.72
280	"	45.63	"	16.97	1.73	52.23	1.815	18.95
300	"	46.40	"	17.26	1.72	53.01	1.8	19.15
320	"	47.08	"	17.51	1.71	53.74	1.79	19.34
340	"	47.69	"	17.74	1.705	54.41	1.78	19.52
360	"	48.24	"	17.94	1.695	55.04	1.775	19.68

TABLE 2  
Totally Real Fields With Small Discriminants

n	Actual lower bound	Unconditional Bound		GRH Bound	
		$\sigma$	$D^{1/n}$	$\sigma$	$D^{1/n}$
3	3.65...	4.195	3.09	5.525	3.23
4	5.18...	2.27	4.21	4.57	4.46
5	6.80...	2.755	5.30	4.04	5.66
6	8.18...	2.435	6.35	3.695	6.82
7	11.05...	2.215	7.33	3.455	7.93

TABLE 3

Totally Complex Fields with Small Discriminants

n	Known Examples	Unconditional Bound		GRH Bound	
		$D^{1/n}$	$\sigma$	$\sigma$	$D^{1/n}$
4	3.28...		4.21	5.565	2.95
8	6.24...		2.57	3.865	5.05
14	8.42...		1.91	3.125	7.20
20	10.90...		1.655	2.81	8.70
28	14.66...		1.49	2.58	10.15
48	16.82...		1.32	2.3	12.47
224	25.71...	Ineq. (1.10)	15.94	1.872	18.25
1332	33.46...	"	20.68	1.821	22.76
8862	39.31...	Ineq. (1.11)	21.62	1.493	25.52
254228	49.10...	"	22.17	1.406	27.69
781420370	74.69...	"	22.19	Ineq. (1.13)	39.67
68733790638	78.64...	"	22.19	"	41.37



TABLE 4  
Lower Bound for Conductors  
 $m = \chi(1)$

$m$	$\chi(g_0) = \chi(1)$		$\chi(g_0) = 0$		$\chi(g_0) = \chi(1)$		$\chi(g_0) = 0$	
	$\sigma$	$F^{1/m}$	$\sigma$	$F^{1/m}$	$\sigma$	$F^{1/m}$	$\sigma$	$F^{1/m}$
2	3.27	4.21	4.21	2.83	4.5	4.46	5.565	2.95
4	1.54	5.86	1.805	3.74	2.635	6.28	2.995	3.91
6	1.275	6.47	1.4	4.07	2.215	7.02	7.435	4.27
8	1.185	6.74	1.26	4.22	2.025	7.43	2.19	4.45
10	1.135	6.88	1.19	4.30	1.91	7.70	2.045	4.57
12	Ineq.(1.4)	7.06	1.15	4.35	1.835	7.89	1.95	4.65
14	"	7.38	1.125	4.39	1.785	8.04	1.88	4.71
16	"	7.57	Ineq.(1.4)	4.47	1.74	8.15	1.83	4.76
18	"	7.69	"	4.55	1.71	8.25	1.79	4.80
20	"	7.77	"	4.61	1.685	8.33	1.755	4.83

kernel of a representation of degree 2 and conductor 283 constructed by Tate. The remaining values (for  $n \geq 224$ ) are derived from the Hilbert class fields of the cyclotomic fields  $\mathbb{Q}(\zeta_p)$ ,  $\zeta_p = e^{2\pi i/p}$ , for  $p = 29, 37, 43, 53, 79$ , and  $83$ , respectively. The Hilbert class field of  $\mathbb{Q}(\zeta_p)$  contains a subfield of degree  $(p-1) h^*(p)$ , where  $h^*(p)$  is the first factor of the class number of  $\mathbb{Q}(\zeta_p)$ , and these are the fields used in the table. (For a table of  $h^*(p)$ , see [9].) These last examples are especially interesting, since the only previous examples of fields of high degree and low discriminant were derived from infinite Hilbert class field towers [10], and the values of  $D^{1/n}$  there were much higher.

The bounds of Table 4 for the conductor  $F = F(\chi)$  of a character  $\chi$  assume that  $L(s, \chi\bar{\chi})$  is analytic for  $s \neq 1$  and that  $\chi$  is irreducible. Theorem 1 is used to estimate  $F(\chi\bar{\chi})$ , and then Lemma 1 is used to bound  $F(\chi)$ .

Acknowledgments

Part of this work was done at the Massachusetts Institute of Technology, with the support of the Hertz Foundation. The author should like to acknowledge the extensive help of J.-P. Serre, on whose observations most of this note is based.

## REFERENCES

1. N.C. Ankeny, S. Chowla, and H. Hasse, On the class number of the maximal real subfield of a cyclotomic field, J. reine angew. Math. 217 (1965), 217-220. MR30 # 3078.
2. E. Artin, "The Collected Papers of Emil Artin" (S. Lang and J. Tate, eds. ), Addison-Wesley 1965.
3. H. Bauer, Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper, J. Number Theory 1 (1969), 161-162. MR 39 # 1426.
4. H. Cohn, A numerical study of Weber's real class number calculation, Numer. Math. 2 (1960), 347-362. MR 23 # A142.
5. E. Landau, "Handbuch der Lehre von der Verteilung der Primzahlen", second ed., Chelsea 1953.
6. ———, "Über die Klassenzahl imaginär - quadratischen Zahlkörper", Gött. Nachr. (1918), 285-295.
7. ———, Zur Theorie der Heckeschen Zeta-funktionen, welche Komplexen Charakteren entsprechen, Math. Z. 4 (1919), 152-162.

8. W. Narkiewicz, "Elementary and Analytic Theory of Algebraic Numbers," (Monografie Matematyczne, No. 57), Polish Scientific Publishers (PWN), Warsaw 1974.
9. M. Newman, A table of the first factor for prime cyclotomic fields, Math. Comp. 24 (1970), 215-219. MR 41 ~~#~~ 1684.
10. A.M. Odlyzko, Lower bounds for discriminants of number fields, to appear in Acta Arith.
11. \_\_\_\_\_, Some analytic estimates of class numbers and discriminants, Inventiones math. 29 (1975), 275-286.
12. \_\_\_\_\_, Lower bounds for discriminants of number fields II, to appear in Tohoku Math. J.
13. M. Pohst, The minimum discriminant of seventh degree totally real algebraic number fields, to appear in J. Number Theory.
14. H.M. Stark, Some effective cases of the Brauer-Siegel Theorem, Inventiones Math. 23 (1974), 135-152.
15. H. Weber, "Lehrbuch der Algebra," 3rd ed., (Chelsea reprint).



# Effective Versions of the Chebotarev Density Theorem

J.C. Lagarias and A.M. Odlyzko

## §1. Introduction

Let  $K$  be an algebraic number field (finite extension of the rationals  $\mathbb{Q}$ ) and  $L$  a normal extension of  $K$  with Galois group  $G = G(L/K)$ . Let  $d_L$  and  $d_K$  denote the absolute values of the discriminants of  $L$  and  $K$ , respectively, and let  $n_L = [L:\mathbb{Q}]$ ,  $n_K = [K:\mathbb{Q}]$ . Throughout this paper  $\mathfrak{p}$  will denote a prime ideal of  $K$  and  $\mathfrak{P}$  a prime ideal of  $L$ . If  $\mathfrak{p}$  is a prime ideal of  $K$  which is unramified in  $L$ , then we use the Artin symbol  $\left[ \frac{L/K}{\mathfrak{p}} \right]$  to denote the conjugacy class of Frobenius automorphisms corresponding to prime ideals  $\mathfrak{P}|\mathfrak{p}$ . For each conjugacy class  $C$  of  $G$ , we define

$$\pi_C(x, L/K) = |\{ \mathfrak{P}; \mathfrak{P} \text{ unramified in } L, \left[ \frac{L/K}{\mathfrak{P}} \right] = C, N_{K/\mathbb{Q}} \mathfrak{p} \leq x \}|.$$

The Chebotarev density theorem [15] asserts that

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|} \text{Li}(x) \quad \text{as } x \rightarrow \infty, \quad (1.1)$$

where  $\text{Li}(x)$  is the familiar logarithmic integral

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \quad \text{as } x \rightarrow \infty.$$

The Chebotarev density theorem generalizes many of the classical results on the distribution of primes and prime ideals. For example, if we consider the trivial extension  $L = K$  of  $K$  ( $K$  does not have to be normal over  $\mathbb{Q}$ ), then there is only one conjugacy class, and (1.1) shows that the number of prime ideals of  $K$  with norm  $\leq x$  is asymptotic to  $\text{Li}(x)$ , which is exactly the prime ideal theorem. If we let  $K = \mathbb{Q}$  and  $L = \mathbb{Q}(e^{2\pi i/q})$ , then the conjugacy classes of  $G$  correspond to the residue classes modulo  $q$ , and (1.1) gives us the prime number theorem for arithmetic progressions.

One of the most important of the many applications of the Chebotarev density theorem deals with the group of an equation. Suppose that  $f(x)$  is a monic polynomial whose coefficients are algebraic integers in  $K$  and which is irreducible over  $K$ . Suppose further that  $L$  is the splitting field of  $f(x)$  over  $K$ . If we regard  $G = G(L/K)$  as a permutation group acting on the roots of  $f(x)$ , then for almost all prime ideals  $\mathcal{P}$  of  $K$  the cycle structure of  $\left[ \frac{L/K}{\mathcal{P}} \right]$  depends on the factorization of  $f(x)$  modulo  $\mathcal{P}$ , and vice



versa. Thus if  $G$  is known, then the Chebotarev density theorem tells us how often various factorizations occur as  $P$  runs through all the prime ideals of  $K$ . On the other hand, if we do not know  $G$ , then factoring  $f(x)$  modulo the prime ideals of  $K$  will yield the complete cycle structures of  $G$ , since by (1.1) for every conjugacy class  $C$  there are infinitely many primes  $P$  with  $\left[ \frac{L/K}{P} \right] = C$ . This can be very helpful in the determination of  $G$  [16; vol. 1, pp. 189-192], especially since by considering enough primes we can even determine the relative densities of elements of  $G$  which have a given cycle structure.

(Unfortunately, sometimes this is not enough to determine  $G$  completely, since it is possible to construct two nonisomorphic groups which have transitive permutation representations in which the number of elements with a given cycle structure is the same for both groups.) In these situations it is important to be able to compute a bound below which every conjugacy class will occur as the Artin symbol of a prime ideal of  $K$ .

The usual proofs of the Chebotarev theorem contain either no error estimates at all, or else estimates which contain constants depending in some undetermined way on the

fields  $K$  and  $L$ . In particular, such estimates do not allow us to specify effectively a value  $x_0 = x_0(L/K)$  such that

$$\pi_C(x, L/K) > 0 \quad \text{if} \quad x \geq x_0. \quad (1.2)$$

The purpose of this paper is to prove two versions of the Chebotarev theorem, each of which has an error term which is an explicit and effectively computable function of  $x$ ,  $n_L$ ,  $d_L$ , and  $|C|/|G|$ . One version assumes the truth of the Generalized Riemann Hypothesis (GRH) and the other holds unconditionally.

We first state the conditional result.

Theorem 1.1. There exists an effectively computable positive absolute constant  $c_1$  such that if the GRH holds for the Dedekind zeta function of  $L$ , then for every  $x > 2$ ,

$$\left| \pi_C(x, L/K) - \frac{|C|}{|G|} \text{Li}(x) \right| \leq c_1 \left\{ \frac{|C|}{|G|} x^{\frac{1}{2}} \log(d_L x^{n_L}) + \log d_L \right\}. \quad (1.3)$$

This theorem yields immediately a value of  $x_0$  such that (1.2) holds. [We utilize here the estimate  $n_L^{-1} \log d_L > 1 + \varepsilon$  for some  $\varepsilon > 0$ , valid for  $n_L > 1$ . It follows from Minkowski's discriminant bound, and it can also be

derived from (5.11) (see [11]).]

Corollary 1.2 There exists an effectively computable positive absolute constant  $c_2$  such that if the GRH holds for the Dedekind zeta function of  $L \neq \mathbb{Q}$ , then for every conjugacy class  $C$  of  $G$  there exists an unramified prime ideal  $P$  in  $K$  such that  $\left[ \frac{L/K}{P} \right] = C$  and

$$N_{K/\mathbb{Q}} P \leq c_2 (\log d_L)^2 (\log \log d_L)^4. \quad (1.4)$$

(If  $L = \mathbb{Q}$ ,  $P = (2)$  yields a solution.)

At the end of this paper we will indicate how the above estimate can be improved so as to eliminate the  $\log \log d_L$  term.

We next state the unconditional result.

Theorem 1.3. If  $n_L > 1$  then  $\zeta_L(s)$  has at most one zero in the region defined by  $s = \sigma + it$  with

$$1 - (4 \log d_L)^{-1} \leq \sigma \leq 1, \quad |t| \leq (4 \log d_L)^{-1}. \quad (1.5)$$

(If  $n_L = 1$ ,  $L = \mathbb{Q}$  and there is no zero in  $|t| \leq 14$ ,  $\sigma > 0$ .)

If such a zero exists, it must be real and simple, and we denote it by  $\beta_0$ .

Further, there exist absolute effectively computable constants  $c_3$  and  $c_4$  such that if

$$x \geq \exp(10n_L(\log d_L)^2), \quad (1.6)$$

then

$$\left| \pi_C(x) - \frac{|C|}{|G|} \text{Li}(x) \right| \leq \frac{|C|}{|G|} \text{Li}(x^{\beta_0}) + c_3 x \exp(-c_4 n_L^{-\frac{1}{2}} (\log x)^{\frac{1}{2}}), \quad (1.7)$$

where the  $\beta_0$  term is present only when  $\beta_0$  exists.

Because of the presence of the  $\beta_0$  factor, Theorem 1.3 does not fully meet our criterion of effectiveness, which is that the error term should depend only on  $x$ ,  $n_L$ ,  $d_L$ , and  $|C|/|G|$ . However, this defect can be remedied by utilizing any effective bound for  $\beta_0$ . In most cases the best known such bound is that of Stark [13; p.148], which we quote below.

Theorem 1.4 Let the notation be as in Theorem 1.3, and let  $m_L = 4$  if  $L$  is normal over  $\mathbb{Q}$ ,  $m_L = 16$  if there is a sequence of fields  $\mathbb{Q} = k_0 \subset k_1 \subset \dots \subset k_r = L$  with each

field normal over the preceding one, and  $m_L = 4n_L!$  otherwise. Then there exists an effectively computable absolute constant  $c_5$  such that

$$\beta_0 < \max \left[ 1 - (m_L \log d_L)^{-1}, 1 - (c_5 d_L^{1/n_L})^{-1} \right]. \quad (1.8)$$

Even if  $\beta_0$  does not exist, Theorem 1.3 does not give a good unconditional bound for the smallest norm of a prime ideal whose Artin symbol is a given conjugacy class. A reasonable conjecture might be that there should be an effectively computable absolute constant  $c$  such that for every normal extension  $L/K$  and every conjugacy class  $C$  of  $G(L/K)$ , there should be an unramified  $P$  with  $\left[ \frac{L/K}{P} \right] = C$  and

$$N_{K/Q} P \leq (\log d_L)^c. \quad (1.9)$$

When  $L$  is a cyclotomic extension of  $K = \mathbb{Q}$ , (1.9) is equivalent to Linnik's theorem [1; p. 39]. However, if  $K = \mathbb{Q}$  and  $L = \mathbb{Q}(\sqrt{d})$  is a quadratic extension of  $\mathbb{Q}$ , the determination of the least prime  $p$  with  $\left[ \frac{L/Q}{(p)} \right] \neq \{1\}$  corresponds to the problem of determining the least quadratic nonresidue (mod  $d$ ), and for this problem no

unconditional bound better than

$$p \leq c_6 d_L^{c_7}, \quad (1.10)$$

is known, where  $c_6$  and  $c_7$  are positive constants. Thus without some major new ideas it would probably be very difficult to prove an unconditional result as good as (1.9). However, by using slightly different techniques (which are designed to detect prime ideals rather than estimate their total number) one can prove the following result [7].

Theorem There exist effectively computable positive absolute constants  $b_1$  and  $b_2$  such that for every conjugacy class  $C$  of  $G$  there exists an unramified prime ideal  $P$  of  $K$  such that  $\left[ \frac{L/K}{P} \right] = C$  and

$$N_{K/Q} P \leq b_1 d_L^{b_2}.$$

The approach used in this paper has a long history.

The argument given here may be viewed as a direct descendent

of de la Vallee Poussin's proof of the prime number theorem. We follow closely the pattern of Davenport's treatment [2] of the prime number theorem for arithmetic progressions. The main innovation here is the careful treatment of the dependencies of various constants on  $n_L$  and  $d_L$  (cf. [2, 4, 5, 8, 10]).

Aside from some slight acquaintance with algebraic and analytic number theory, this paper also assumes knowledge of the basic properties of Hecke and Artin L-functions [6]. The deepest of these results is the abelian reciprocity law, which tells us that an abelian Artin L-series is a Hecke L-series, and so is analytic for  $s \neq 1$ .

Throughout this paper  $c_1, c_2, \dots$  will denote effectively computable positive absolute constants. (In particular, they are independent of  $K$  and  $L$ .) The Vinogradov notation

$$f \ll g$$

will be used to denote the existence of an effectively computable positive absolute constant  $A$  (not necessarily the same in each occurrence) such that

$$|f| \leq Ag,$$

in the range indicated.



## §2. Outline of the main argument

The main argument is primarily concerned with the derivation of an asymptotic formula with an explicit error term for a weighted prime-power-counting function  $\psi_C(x) = \psi_C(x, L/K)$  associated to  $\pi_C(x, L/K)$ . It is defined by

$$\psi_C(x, L/K) = \sum_{\substack{N_{K/Q} p^m \leq x \\ p \text{ unramified} \\ \left[ \frac{L/K}{p} \right]^m = C}} \log(N_{K/Q} p).$$

The details of this argument are complicated, but the main steps are simple in conception:

- (i)  $\psi_C(x)$  differs from a truncated inverse Mellin transform

$$I_C(x, T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} F_C(s) \frac{x^s}{s} ds,$$

by a remainder term  $R_1(x, T)$ .

- (ii)  $F_C(s)$  can in fact be written as a linear combination of logarithmic derivatives of Hecke (abelian) L-functions. As a consequence, all the singularities of  $F_C(s)$ ,

which are simple poles only, occur at the zeroes and pole of  $\zeta_L(s)$ .

- (iii)  $I_C(x, T)$  differs from a certain contour integral

$$B_C(x, T) = \frac{1}{2\pi i} \oint_{B_T} F_C(s) \frac{x^s}{s} ds ,$$

by a remainder term  $R_2(x, T)$ . This step is traditionally labelled "shifting the line of integration to the left."

Certain results on the density of zeroes of  $\zeta_L(s)$  in the critical strip  $0 < \operatorname{Re} s < 1$  are necessary to estimate  $R_2(x, T)$ .

- (iv) The contour integral  $B_C(x, T)$  is evaluated by Cauchy's residue theorem. The integrand has poles at the zeroes and the pole of  $\zeta_L(s)$ , and the result is a main term  $\frac{|C|}{|G|} x$  coming from the pole of  $\zeta_L(s)$  at  $s = 1$ , together with a certain sum  $S(x, T)$  over the zeroes of  $\zeta_L(s)$  within the contour  $B_T$ .

The end result of these steps is a truncated "explicit formula" for  $\psi_C(x)$  with

an unconditional error term, which is stated as Theorem 7.1.

- (v) The sum over the zeroes  $S(x, T)$  is estimated. It is at this point that unproved hypotheses about the zeroes can be helpful. An unconditional upper bound for  $|S(x, T)|$  is obtained using the existence of a zero-free region of  $\zeta_L(s)$  near the vertical line  $\sigma = 1$ . A much better estimate for  $|S(x, T)|$  is made assuming the Generalized Riemann Hypothesis for  $\zeta_L(s)$ .
- (vi) The asymptotic formula  $\psi_C(x) \sim \frac{|C|}{|G|} x$  with an explicit remainder term is derived by making an appropriate choice of  $T$  as a function of  $x$ , to minimize the accumulated error terms. (This choice depends on whether the GRH is assumed or not, of course.)
- (vii) The asymptotic formula  $\pi_C(x) \sim \frac{|C|}{|G|} \text{Li}(x)$  with an explicit remainder term is derived by partial summation from that for  $\psi_C(x)$ .

The remaining sections of this paper carry out the details (although we will not follow this outline exactly).

### §3. Artin L-functions and Mellin transforms

In this section we establish the relation between  $\psi_C(x)$  and a certain truncated inverse Mellin transform. Throughout this and subsequent sections we will use the abbreviations  $\pi_C(x)$ ,  $\psi_C(x)$ , and  $N$  for  $\pi_C(x, L/K)$ ,  $\psi_C(x, L/K)$ , and  $N_{K/Q}$ , respectively. We will also use  $\phi$  to denote irreducible characters of  $G = G(L/K)$ .

For each irreducible character  $\phi$  of  $G$  we define

$$\phi_K(P^m) = \frac{1}{e} \sum_{\alpha \in I} \phi(\tau^m \alpha), \quad (3.1)$$

where  $I$  is the inertia group of  $P$ , one of the prime ideal factors of  $P$ ,  $e = |I|$ , and  $\tau$  is one of the Frobenius automorphisms corresponding to  $P$ . If  $L(s, \phi, L/K)$  is the Artin L-series associated to  $\phi$ , then for  $\text{Re}(s) > 1$  we have

$$-\frac{L'}{L}(s, \phi, L/K) = \sum_P \sum_{m=1}^{\infty} \phi_K(P^m) \log(NP) (NP)^{-ms}, \quad (3.2)$$

where the outer sum is over all the prime ideals of  $K$ . We should also note that the definitions (3.1) and (3.2) apply equally well to reducible characters.

To single out those  $P^m$  with  $\left[\frac{L/K}{P}\right]^m = C$ , we will use the characters  $\phi$ . (Unfortunately this works only to the

extent that some extraneous prime powers  $p^m$  corresponding to  $P$  that ramify in  $L$  are also included.) Suppose that  $g \in C$ . We define a function  $f_C: G \rightarrow \mathbb{C}$  by

$$f_C = \sum_{\phi} \bar{\phi}(g) \phi. \quad (3.3)$$

Then the orthogonality relations for characters imply that

$$f_C(\tau) = \begin{cases} \frac{|G|}{|C|} & \text{if } \tau \in C, \\ 0 & \text{if } \tau \notin C. \end{cases} \quad (3.4)$$

Hence if

$$F_C(s) = - \frac{|C|}{|G|} \sum_{\phi} \bar{\phi}(g) \frac{L'}{L}(s, \phi, L/K), \quad (3.5)$$

then (3.2) through (3.5) show that for  $\text{Re}(s) > 1$  we have the Dirichlet series expansion

$$F_C(s) = \sum_P \sum_{m=1}^{\infty} \theta(P^m) \log(NP) (NP)^{-ms}, \quad (3.6)$$

where for  $P$  unramified in  $L$  we have

$$\theta(P^m) = \begin{cases} 1 & \text{if } \left[ \frac{L/K}{P} \right]^m = C, \\ 0 & \text{otherwise,} \end{cases}$$

and  $|\theta(P^m)| \leq 1$  if  $P$  ramifies in  $L$ .

Equation (3.6) shows that except for the ramified prime factors,  $\psi_C(x)$  is a partial sum of the coefficients of  $F_C(s)$ . To obtain  $\psi_C(x)$  from  $F_C(s)$  we will use the following well-known truncated version of the inverse Mellin transform [14; p. 54], [2; pp. 109-110].

Lemma 3.1. If  $y > 0$ ,  $\sigma > 0$ , and  $T > 0$ , then

$$\left| \frac{1}{2\pi i} \int_{\sigma-iT}^{\sigma+iT} \frac{y^s}{s} ds - 1 \right| \leq y^\sigma \min(1, T^{-1} |\log y|^{-1}) \quad \text{if } y > 1,$$

$$\left| \frac{1}{2\pi i} \int_{\sigma-iT}^{\sigma+iT} \frac{y^s}{s} ds - \frac{1}{2} \right| \leq \sigma T^{-1} \quad \text{if } y = 1,$$

and

$$\left| \frac{1}{2\pi i} \int_{\sigma-iT}^{\sigma+iT} \frac{y^s}{s} ds \right| \leq y^\sigma \min(1, T^{-1} |\log y|^{-1}) \quad \text{if } 0 < y < 1.$$

Let  $\sigma_0 > 1$ ,  $x \geq 2$ , and define

$$I_C(x, T) = \frac{1}{2\pi i} \int_{\sigma_0-iT}^{\sigma_0+iT} F_C(s) \frac{x^s}{s} ds. \quad (3.7)$$

Since the Dirichlet series in (3.6) is absolutely convergent

for  $\operatorname{Re}(s) > 1$ , we can integrate term by term (with the help of Lemma 3.1) to obtain

$$\left| I_C(x, T) - \sum_{\substack{P, m \\ NP^m \leq x}} \theta(P^m) \log NP \right| \leq \sum_{\substack{P, m \\ NP^m = x}} \{ \log NP + \sigma_0 T^{-1} \} + R_0(x, T), \quad (3.8)$$

where

$$R_0(x, T) = \sum_{\substack{P, m \\ NP^m \neq x}} \left( \frac{x}{NP^m} \right)^{\sigma_0} \min(1, T^{-1} \left| \log \frac{x}{NP^m} \right|^{-1}) \log NP \quad (3.9)$$

and where the sum on the right side of (3.8) is present only when there are  $P$  and  $m$  with  $NP^m = x$ . Now the sum on the left side of (3.8) equals  $\psi_C(x)$ , except for the ramified prime terms. However,  $NP \geq 2$  for each prime ideal  $P$ , all the ramified prime ideals  $P$  divide the discriminant of  $L$  over  $K$ , and so

$$\begin{aligned} \left| \sum_{\substack{P, m \\ NP^m \leq x}} \theta(P^m) \log NP - \psi_C(x) \right| &\leq \sum_{\substack{P, m \\ P \text{ ramified} \\ NP^m \leq x}} \log NP \\ &\leq \sum_{\substack{P \\ P \text{ ramified}}} \log NP \sum_{\substack{m \\ NP^m \leq x}} 1 \leq 2 \log x \sum_{\substack{P \\ P \text{ ramified}}} \log NP \\ &\leq 2 \log x \log d_L. \end{aligned}$$



(We should remark that this estimate would be the same even if  $C$  were a union of conjugacy classes.) Also, there are at most  $n_K$  distinct pairs  $P, m$  such that  $NP^m = x$ , and so

$$\sum_{\substack{P, m \\ NP^m = x}} \log NP \leq n_K \log x.$$

Thus (3.8) yields

$$\psi_C(x) = I_C(x, T) + R_1(x, T), \quad (3.10)$$

where

$$R_1(x, T) \leq 2 \log x \log d_L + n_K \sigma_0 T^{-1} + n_K \log x + R_0(x, T). \quad (3.11)$$

The remainder of this section is devoted to establishing an estimate for  $R_0(x, T)$ .

So far we allowed  $\sigma_0$  to be any number  $> 1$ . We now define

$$\sigma_0 = 1 + (\log x)^{-1}. \quad (3.12)$$

While this is only one of many possible choices, it is quite convenient, not least because of the relation  $x^{\sigma_0} = ex$ .

We now write  $R_0(x, T) = S_1 + S_2 + S_3$ , where  $S_1$  consists of those terms of (3.9) for which  $NP^m \leq \frac{3}{4}x$  or  $NP^m \geq \frac{5}{4}x$ ,  $S_2$  of those for which  $|x - NP^m| \leq 1$ , and  $S_3$  of the remaining

ones. If  $NP^m \leq \frac{3}{4}x$  or  $NP^m \geq \frac{5}{4}x$ , then

$$\left| \log \frac{x}{NP^m} \right| \geq \log \frac{5}{4} ,$$

$$\min (1, T^{-1} \left| \log \frac{x}{NP^m} \right|^{-1}) \leq T^{-1} \quad \text{for } T \geq 1,$$

and so

$$\begin{aligned} S_1 &\ll xT^{-1} \sum_{P,m} (NP)^{-m\sigma_0} \log NP \\ &= xT^{-1} \left[ -\frac{\zeta'_K}{\zeta_K}(\sigma_0) \right] . \end{aligned} \quad (3.13)$$

To bound this term we use an auxiliary result.

Lemma 3.2. For  $\sigma > 1$ ,

$$-\frac{\zeta'_K}{\zeta_K}(\sigma) \leq -n_K \frac{\zeta'_Q}{\zeta_Q}(\sigma) .$$

Proof We have

$$-\frac{\zeta'_K}{\zeta_K}(\sigma) = \sum_P \frac{\log NP}{(NP)^\sigma - 1} , \quad -\frac{\zeta'_Q}{\zeta_Q}(\sigma) = \sum_p \frac{\log p}{p^{\sigma-1}} ,$$

where in the second sum  $p$  runs through the rational primes.

Now for each prime ideal  $P$ ,  $NP = p^k$  for some positive integer  $k$ . Thus

$$\frac{\log NP}{(NP)^\sigma - 1} = \frac{k \log p}{p^{k\sigma} - 1} = \frac{k}{p^{(k-1)\sigma} + \dots + 1} \cdot \frac{\log p}{p^\sigma - 1} \leq \frac{\log p}{p^\sigma - 1}.$$

Also, there are at most  $n_K$  distinct  $P$  lying over a given rational prime  $p$ , so that

$$-\frac{\zeta'_K}{\zeta_K}(\sigma) \leq n_K \sum_p \frac{\log p}{p^\sigma - 1} = -n_K \frac{\zeta'_Q}{\zeta_Q}(\sigma), \quad \text{q.e.d.}$$

Since

$$-\frac{\zeta'_Q}{\zeta_Q}(\sigma) \ll (\sigma - 1)^{-1}$$

for  $\sigma > 1$ , Lemma 3.2 and (3.13) show that for  $T \geq 1$ ,

$$S_1 \ll n_K x T^{-1} \log x. \quad (3.14)$$

The second sum  $S_2$  consists of those terms  $P^m$  for which  $0 < |NP^m - x| \leq 1$ . There are at most  $2n_K$  of such  $P^m$  and since

$$\min(1, T^{-1} \left| \log \frac{x}{NP^m} \right|^{-1}) \leq 1,$$

we obtain

$$S_2 \leq 2n_K \log(x+1) \left( \frac{x}{x-1} \right)^{\sigma_0} \ll n_K \log x. \quad (3.15)$$

The final sum  $S_3$  consists of those terms  $P^m$  for which  $1 < |NP^m - x| < \frac{1}{4}x$ . Here we use the estimate

$$\left| \log \frac{x}{n} \right|^{-1} \leq \frac{2n}{|x-n|},$$

valid for  $n \geq \frac{1}{2}x$ , to obtain

$$\begin{aligned} S_3 &\ll T^{-1} \log x \sum_{\substack{n \\ 1 < |n-x| < \frac{1}{4}x}} \left| \log \frac{x}{n} \right|^{-1} \sum_{\substack{p, m \\ Np^m = n}} 1 \\ &\ll n_K x T^{-1} \log x \sum_{1 \leq k < \frac{1}{4}x} \frac{1}{k} \\ &\ll n_K x T^{-1} (\log x)^2. \end{aligned} \quad (3.16)$$

Putting (3.14)-(3.16) together we obtain

$$R_0(x, T) \ll n_K \log x + n_K x T^{-1} (\log x)^2, \quad (3.17)$$

valid for all  $x \geq 2$ ,  $T \geq 1$ . If we now combine (3.17) with (3.11), we obtain finally the estimate

$$R_1(x, T) \ll \log x \log d_L + n_K \log x + n_K x T^{-1} (\log x)^2, \quad (3.18)$$

valid for all  $x \geq 2$ ,  $T \geq 1$ , which was the goal of this section. We should mention here that the  $\log x \log d_L$  term in (3.18) (which came from the ramified primes) would have been the same even if  $C$  were to be the union of any number of conjugacy classes. Let us also note that if

$L \neq \mathbb{Q}$ , then  $n_K \leq n_L \ll \log d_L$ , and so the second term on the right side of (3.18) can be absorbed in the first one.

#### §4. Reduction to the case of Hecke L-functions

Our definition (3.5) of  $F_C(s)$  was in terms of Artin L-functions corresponding to the (usually nonlinear) characters of  $G(L/K)$ . In this section we show that  $F_C(s)$  can be written in terms of Hecke (abelian) L-functions. This will enable us to obtain much better results on the location and density of the singularities of  $F_C(s)$ . The reduction we will use is due to Deuring [3] (later rediscovered by MacCluer [9]). We learned of it from [10], and should like to thank J. -P. Serre for bringing Moreno's paper to our attention and for supplying the following formulation of Deuring's idea.

In defining  $F_C(s)$  by (3.5), we have already selected an element  $g \in C$ . Let  $H = \langle g \rangle$  be the cyclic group generated by  $g$ ,  $E$  the fixed field of  $H$ , and let  $\chi$  denote the irreducible characters of  $H$ . Since  $H$  is cyclic, the characters  $\chi$  are one-dimensional. We will retain this notation for the rest of this paper.

Lemma 4.1. We have

$$F_C(s) = - \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \frac{L'}{L}(s, \chi, L/E). \quad (4.1)$$

Proof Let  $\tau: H \rightarrow \mathbb{C}$  be the class function defined by

$$\tau(h) = \begin{cases} |H| & \text{if } h = g, \\ 0 & \text{if } h \neq g. \end{cases}$$

Then the orthogonality relations for characters of  $H$  imply that

$$\tau = \sum_{\chi} \bar{\chi}(g) \chi.$$

Let  $\tau^*$  denote the class function on  $G$  induced by  $\tau$ , which by direct calculation equals

$$\tau^*(y) = \begin{cases} |C_G(g)| & y \in C, \\ 0 & y \notin C, \end{cases}$$

where  $C_G(g)$  is the centralizer of  $g$  in  $G$ . Now

$|C_G(g)||C| = |G|$  so that  $\tau^* = f_C$  [see (3.4)]. This implies

$$\sum_{\chi} \bar{\chi}(g) \chi^* = \sum_{\phi} \bar{\phi}(g) \phi,$$

so that for  $\operatorname{Re}(s) > 1$  we have

$$F_C(s) = - \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \frac{L'}{L}(s, \chi^*, L/K). \quad (4.2)$$

But  $L(s, \chi^*, L/K) = L(s, \chi, L/E)$ , and so (4.1) holds for  $\operatorname{Re}(s) > 1$ , and therefore (by analytic continuation) for all  $s$ .

### §5. Density of zeroes of Hecke L-functions

We have now shown that for  $x \geq 2$  and  $T \geq 1$ , say,

$$\psi_C(x) = I_C(x, T) + R_1(x, T),$$

where  $R_1(x, T)$  satisfies (3.18) and

$$I_C(x, T) = - \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{L'}{L}(s, \chi, L/E) ds, \quad (5.1)$$

where  $\sigma_0 = 1 + (\log x)^{-1}$  and  $\chi$  runs through the (one-dimensional) irreducible characters of  $H = \langle g \rangle$ . Our next goal will be to evaluate each of the integrals in (5.1).

[This turns out to be more convenient than integrating  $F_C(s)$ .] To accomplish this we will need some upper bounds on the number of singularities of  $L'/L$ .

Since  $L$  and  $E$  are going to be fixed from now on, we



will use  $L(s, \chi)$  to denote  $L(s, \chi, L/E)$ . Also, we let  $F(\chi)$  denote the conductor of  $\chi$  and set

$$A(\chi) = d_{E/Q}^{N_E} (F(\chi)) \quad (5.2)$$

and

$$\delta(\chi) = \begin{cases} 1 & \text{if } \chi = \chi_1, \text{ the principal character,} \\ 0 & \text{otherwise.} \end{cases} \quad (5.3)$$

We recall that for each  $\chi$  there exist non-negative integers  $a = a(\chi)$ ,  $b = b(\chi)$  such that

$$a(\chi) + b(\chi) = n_E, \quad (5.4)$$

and such that if we define

$$\gamma_\chi(s) = \left[ \pi^{-\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right) \right]^b \left[ \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \right]^a \quad (5.5)$$

and

$$\xi(s, \chi) = [s(s-1)]^{\delta(\chi)} A(\chi)^{s/2} \gamma_\chi(s) L(s, \chi), \quad (5.6)$$

then  $\xi(s, \chi)$  satisfies the functional equation

$$\xi(1-s, \bar{\chi}) = W(\chi) \xi(s, \chi), \quad (5.7)$$

where  $W(\chi)$  is a certain constant of absolute value 1.

Furthermore,  $\xi(s, \chi)$  is an entire function of order 1 and does not vanish at  $s = 0$ , and hence by the Hadamard

product theorem we have

$$\xi(s, \chi) = e^{B_1(\chi) + B(\chi)s} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho} \quad (5.8)$$

for some constants  $B_1(\chi)$  and  $B(\chi)$ , where  $\rho$  runs through all the zeroes of  $\xi(s, \chi)$ , which are precisely those zeroes  $\rho = \beta + i\gamma$  of  $L(s, \chi)$  for which  $0 < \beta < 1$  [the so-called "nontrivial zeroes" of  $L(s, \chi)$ ]. [We recall that  $L(s, \chi)$  and hence  $\xi(s, \chi)$  have no zeroes  $\rho$  with  $\operatorname{Re}(\rho) \geq 1$ .] From now on  $\rho$  will denote nontrivial zeroes of  $L(s, \chi)$ .

Since we are interested in the integrals in (5.1), which involve  $L'/L$ , we differentiate (5.6) and (5.8) logarithmically to obtain the important identity

$$\begin{aligned} \frac{L'}{L}(s, \chi) &= B(\chi) + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2} \log A(\chi) \\ &\quad - \delta(\chi) \left[\frac{1}{s} + \frac{1}{s-1}\right] - \frac{\gamma'_\chi}{\gamma_\chi}(s), \end{aligned} \quad (5.9)$$

valid identically in the complex variable  $s$ . A difficulty in the use of this formula is caused by the presence of the constant  $B(\chi)$ , which depends in an as-yet-undetermined way on  $\chi$ . However, since  $(s-1)^{\delta(\chi)} L(s, \chi)$  is entire, the functional equation (5.7) easily implies the

following result, which is proved in [11].

Lemma 5.1. With notation as above,

$$\operatorname{Re} B(\chi) = - \sum_{\rho} \operatorname{Re} \frac{1}{\rho}, \quad (5.10)$$

and

$$\begin{aligned} \frac{L'}{L}(s, \chi) + \frac{L'}{L}(s, \bar{\chi}) &= \sum_{\rho} \left( \frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}} \right) - \log A(\chi) \\ &\quad - 2\delta(\chi) \left( \frac{1}{s} + \frac{1}{s-1} \right) - 2 \frac{\gamma'_{\chi}}{\gamma_{\chi}}(s) \end{aligned} \quad (5.11)$$

holds identically in the complex variable  $s$ , where  $\rho$  runs through the nontrivial zeroes of  $L(s, \chi)$ .

This lemma will enable us to obtain estimates both of  $B(\chi)$  and of the density of zeroes of  $L(s, \chi)$ . We should mention, however, that an analog of the above lemma could be proved for general Artin  $L$ -functions, but it would contain sums over the possible poles of such  $L$ -functions, and these pole terms would prevent us from obtaining an estimate as good as the one below. The purpose of the preceding section's reduction to the case of abelian  $L$ -function was to avoid these difficulties.

We first derive some easy auxiliary results.

Lemma 5.2. If  $\sigma = \operatorname{Re}(s) > 1$ , then

$$\left| \frac{L'}{L}(s, \chi) \right| \ll \frac{n_E}{\sigma-1}.$$

Proof A comparison of the Dirichlet series shows that

$$\left| \frac{L'}{L}(s, \chi) \right| \leq - \frac{\zeta'_E}{\zeta_E}(\sigma),$$

and the result follows from Lemma 3.2.

Lemma 5.3. If  $\sigma = \operatorname{Re}(s) > -1/2$  and  $|s| \geq 1/8$ , then

$$\left| \frac{\gamma'_\chi}{\gamma_\chi}(s) \right| \ll n_E \log(|s| + 2).$$

Proof This lemma follows from the definition of  $\gamma_\chi(s)$  and the fact that

$$\frac{\Gamma'}{\Gamma}(z) \ll \log(|z| + 2)$$

for  $z$  satisfying  $|z| \geq 1/16$ ,  $\operatorname{Re} z > -1/4$  [17; p.251] (cf. Lemma 6.1).

We now come to the main result of this section. We let  $n_\chi(t)$  denote the number of zeroes  $\rho = \beta + i\gamma$  of  $L(s, \chi)$

with  $0 < \beta < 1$ ,  $|\gamma - t| \leq 1$ .

Lemma 5.4. For all  $t$  we have

$$n_{\chi}(t) \ll \log A(\chi) + n_E \log(|t| + 2) \quad (5.12)$$

Proof We evaluate (5.11) at  $s = 2 + it$ . Lemmas 5.2 and 5.3 imply that

$$\sum_{\rho} \operatorname{Re}\left(\frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}}\right) \ll \log A(\chi) + n_E \log(|t| + 2). \quad (5.13)$$

But  $\operatorname{Re}(s-\rho)^{-1} > 0$  and  $\operatorname{Re}(s-\bar{\rho})^{-1} > 0$  since  $2 = \operatorname{Re}(s) > \operatorname{Re}(\rho)$ ,

so

$$\begin{aligned} \sum_{\rho} \operatorname{Re}\left(\frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}}\right) &\geq \sum_{\substack{\rho \\ |\gamma-t| \leq 1}} \frac{2-\beta}{(2-\beta)^2 + (t-\gamma)^2} \\ &\geq \sum_{\substack{\rho \\ |\gamma-t| \leq 1}} \frac{1}{5} = \frac{1}{5} n_{\chi}(t), \end{aligned}$$

since  $1 < 2 - \beta < 2$ , which proves the lemma.

The bound (5.12) (which is essentially best possible) will be crucial in many of our subsequent arguments. In the case of general Artin L-functions, we could obtain an

estimate similar to (5.13), but it would be for the difference of a sum over the zeroes and a similar sum over the poles and the real part of the poles' contribution would be negative.

We now utilize Lemma 5.4 to obtain two additional auxiliary results. We first show that  $B(\chi)$  depends mostly on the very small zeroes of  $L(s, \chi)$ .

Lemma 5.5. For any  $\varepsilon$  with  $0 < \varepsilon \leq 1$  we have

$$B(\chi) + \sum_{\substack{\rho \\ |\rho| < \varepsilon}} \frac{1}{\rho} \ll \varepsilon^{-1} (\log A(\chi) + n_E).$$

Proof Set  $s = 2$  in (5.9) and use lemmas 5.2 and 5.3 to estimate the  $L(s, \chi)$  and  $\gamma_\chi$  terms, respectively. We obtain

$$B(\chi) + \sum_{\rho} \left( \frac{1}{2-\rho} + \frac{1}{\rho} \right) \ll \log A(\chi) + n_E.$$

Now

$$\left| \frac{1}{2-\rho} + \frac{1}{\rho} \right| = \frac{2}{|\rho(2-\rho)|} \leq \frac{2}{|\rho|^2},$$

and so Lemma 5.4 implies

$$\sum_{|\rho| \geq 1} \left| \frac{1}{2-\rho} + \frac{1}{\rho} \right| \ll \sum_{j=1}^{\infty} \frac{n_\chi(j)}{j^2} \ll \log A(\chi) + n_E.$$

Also,  $|2-\rho| \geq 1$ , so

$$\sum_{|\rho| < 1} \left| \frac{1}{2-\rho} \right| \ll \log A(\chi) + n_E,$$

and hence

$$B(\chi) + \sum_{\substack{\rho \\ |\rho| < \varepsilon}} \frac{1}{\rho} \ll \sum_{\substack{\rho \\ \varepsilon \leq |\rho| < 1}} \frac{1}{|\rho|} + \log A(\chi) + n_E,$$

which together with Lemma 5.4 completes the proof.

Lemma 5.6. If  $s = \sigma + it$  with  $-1/2 \leq \sigma \leq 3$ ,  $|s| \geq 1/8$ , then

$$\left| \frac{L'}{L}(s, \chi) + \frac{\delta(\chi)}{s-1} - \sum_{\substack{\rho \\ |\gamma-t| \leq 1}} \frac{1}{s-\rho} \right| \ll \log A(\chi) + n_E \log(|t| + 2).$$

Proof We evaluate (5.9) at  $\sigma + it$  and  $3 + it$  and subtract the resulting relations [in order to eliminate  $B(\chi)$ ] to obtain

$$\begin{aligned} \frac{L'}{L}(s, \chi) - \frac{L'}{L}(3+it, \chi) &= \sum_{\rho} \left( \frac{1}{s-\rho} - \frac{1}{3+it-\rho} \right) - \frac{\gamma'_\chi}{\gamma_\chi}(s) \\ &\quad + \frac{\gamma'_\chi}{\gamma_\chi}(3+it) - \delta(\chi) \left( \frac{1}{s} + \frac{1}{s-1} - \frac{1}{2+it} - \frac{1}{3+it} \right). \end{aligned}$$



We now use Lemmas 5.2 and 5.3 to estimate the  $L(3+it, \chi)$  and the gamma factors, respectively. We discover that

$$\begin{aligned} & \left| \frac{L'}{L}(s, \chi) + \frac{\delta(\chi)}{s-1} - \sum_{\substack{\rho \\ |\gamma-t| \leq 1}} \frac{1}{s-\rho} \right| \\ & \ll n_E \log(|t|+2) + \sum_{\substack{\rho \\ |\gamma-t| > 1}} \left| \frac{1}{s-\rho} - \frac{1}{3+it-\rho} \right| \\ & \quad + \sum_{\substack{\rho \\ |\gamma-t| \leq 1}} \left| \frac{1}{3+it-\rho} \right|. \end{aligned} \quad (5.14)$$

Since  $|3+it-\rho| > 1$  for all  $\rho$  and there are  $n_\chi(t)$  terms in the last sum, it is  $\ll \log A(\chi) + n_E \log(|t| + 2)$ . For the first sum on the right side of (5.14) we have

$$\begin{aligned} \sum_{\substack{\rho \\ |\gamma-t| > 1}} \left| \frac{1}{s-\rho} - \frac{1}{3+it-\rho} \right| &= \sum_{\substack{\rho \\ |\gamma-t| > 1}} \frac{3-\sigma}{|s-\rho| |3+it-\rho|} \\ &\ll \sum_{j=1}^{\infty} \frac{n_\chi(t+j) + n_\chi(t-j)}{j^2} \\ &\ll \log A(\chi) + n_E \log(|t| + 2), \end{aligned}$$

and this proves the lemma.

§6. The contour integral

The next step in the proof is to evaluate  $I_C(x, T)$  by evaluating

$$I_\chi(x, T) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} \frac{L'}{L}(s, \chi) ds \quad (6.1)$$

for each character  $\chi$  of  $H = \langle g \rangle$ . So far the only condition on  $T$  was  $T \geq 1$ . We now impose the additional requirement that  $T$  should not coincide with the ordinate of a zero of any of the  $L(s, \chi)$ . We also introduce a new parameter,  $U$ , which will satisfy  $U = j + 1/2$  for some non-negative integer  $j$  (eventually we will let  $U \rightarrow \infty$ ) and define

$$I_\chi(x, T, U) = \frac{1}{2\pi i} \int_{B_{T,U}} \frac{x^s}{s} \frac{L'}{L}(s, \chi) ds, \quad (6.2)$$

where  $B_{T,U}$  is the positively oriented rectangle with vertices at  $\sigma_0 - iT$ ,  $\sigma_0 + iT$ ,  $-U + iT$ , and  $-U - iT$ . Now  $I_\chi(x, T, U)$  can easily be evaluated exactly in terms of the singularities of the integrand as we will show in the next section. In this section we will show that

$$R_\chi(x, T, U) = I_\chi(x, T, U) - I_\chi(x, T) \quad (6.3)$$

is small.

The remainder  $R_\chi(x, T, U)$  may be divided into the

vertical integral

$$V_{\chi}(x, T, U) = \frac{1}{2\pi} \int_T^{-T} \frac{x^{-U+it}}{-U+it} \frac{L'}{L}(-U+it, \chi) dt \quad (6.4)$$

and the two horizontal integrals

$$H_{\chi}(x, T, U) = \frac{1}{2\pi i} \int_{-U}^{-1/4} \left\{ \frac{x^{\sigma-iT}}{\sigma-iT} \frac{L'}{L}(\sigma-iT, \chi) - \frac{x^{\sigma+iT}}{\sigma+iT} \frac{L'}{L}(\sigma+iT, \chi) \right\} d\sigma, \quad (6.5)$$

$$H_{\chi}^*(x, T) = \frac{1}{2\pi i} \int_{-1/4}^0 \left\{ \frac{x^{\sigma-iT}}{\sigma-iT} \frac{L'}{L}(\sigma-iT, \chi) - \frac{x^{\sigma+iT}}{\sigma+iT} \frac{L'}{L}(\sigma+iT, \chi) \right\} d\sigma. \quad (6.6)$$

$V_{\chi}$  and  $H_{\chi}$  will be estimated by using Lemma 6.2 to bound  $L'/L$ . First, however, we prove an auxiliary result about the digamma function.

Lemma 6.1. If  $|z + k| \geq 1/8$  for all non-negative integers  $k$ , then

$$\frac{\Gamma'}{\Gamma}(z) \ll \log(|z| + 2).$$

Proof If  $\operatorname{Re} z \geq 1$ , this is well-known [17, p.251]. If  $\operatorname{Re} s < 1$ , then the recurrence relation

$$\frac{\Gamma'}{\Gamma}(u) = \frac{\Gamma'}{\Gamma}(u+1) - \frac{1}{u}$$

iterated  $m$  times shows that

$$\frac{\Gamma'}{\Gamma}(z) = \frac{\Gamma'}{\Gamma}(z+m) - \sum_{k=0}^{m-1} \frac{1}{z+k}$$

for any positive integer  $m$ . Choose  $m = [|z| + 2]$ . Then

$\operatorname{Re}(z+m) > 1$ , so that

$$\frac{\Gamma'}{\Gamma}(z+m) \ll \log(|z| + 2),$$

while  $|z+k| \geq 1/8$  for all non-negative integers  $k$  implies

$$\sum_{k=0}^{m-1} \frac{1}{z+k} \ll \sum_{k=0}^{m-1} \frac{1}{k + 1/8} \ll \log(|z| + 2),$$

which proves the lemma.

Lemma 6.2. If  $s = \sigma + it$  with  $\sigma \leq -1/4$ , and  $|s+m| \geq 1/4$  for all non-negative integers  $m$ , then

$$\frac{L'}{L}(s, \chi) \ll \log A(\chi) + n_E \log(|s| + 2).$$

Proof The functional equation (5.7) and the definitions (5.5) and (5.6) imply that

$$\frac{L'}{L}(s, \chi) = -\frac{L'}{L}(1-s, \bar{\chi}) - \log A(\chi) - \frac{\gamma_{\chi}'}{\gamma_{\chi}}(1-s) - \frac{\gamma_{\chi}'}{\gamma_{\chi}}(s). \quad (6.7)$$

Since  $\operatorname{Re}(1-s) \geq 5/4$ , we can use Lemma 5.2 to bound  $(L'/L)(1-s, \bar{\chi})$ . The lemma then follows by an application of Lemma 6.1 to estimate the  $\gamma_\chi$  terms.

Estimates for  $V_\chi(x, T, U)$  and  $H_\chi(x, T, U)$  are now very easy to obtain. By the above lemma we have the crude estimates ( $U = j + 1/2$  so that  $|-U+it+m| \geq 1/4$  for all integers  $m$ )

$$\begin{aligned} V_\chi(x, T, U) &\ll \frac{x^{-U}}{U} \int_{-T}^T \left| \frac{L'}{L}(-U+it, \chi) \right| dt \\ &\ll \frac{x^{-U}}{U} T \{ \log A(\chi) + n_E \log(T+U) \}, \end{aligned} \quad (6.8)$$

and

$$\begin{aligned} H_\chi(x, T, U) &\ll \int_{-\infty}^{-1/4} \frac{x^\sigma}{T} (\log A(\chi) + n_E \log(|\sigma| + 2) + n_E \log T) d\sigma \\ &\ll \frac{x^{-1/4}}{T} \{ \log A(\chi) + n_E \log T \}. \end{aligned} \quad (6.9)$$

Better estimates can easily be obtained, but would not be too significant, since other error terms will be much larger.

It remains to estimate  $H_\chi^*(x, T)$ . Lemma 5.6 shows that

$$\frac{L'}{L}(\sigma+iT, \chi) - \sum_{\substack{\rho \\ |\gamma-T| \leq 1}} \frac{1}{\sigma+iT-\rho} \ll \log A(\chi) + n_E \log T$$

if  $-1/4 \leq \sigma \leq \sigma_0 = 1 + (\log x)^{-1}$ ,  $x \geq 2$ ,  $T \geq 2$ , and a similar estimate holds for  $L'/L$  at  $\sigma - iT$ . Therefore,

$$\begin{aligned}
 H_{\chi}^*(x, t) &= \frac{1}{2\pi i} \int_{-1/4}^{\sigma_0} \left\{ \frac{x^{\sigma-iT}}{\sigma-iT} \sum_{\substack{\rho \\ |\gamma+T| \leq 1}} \frac{1}{\sigma-iT-\rho} \right. \\
 &\quad \left. - \frac{x^{\sigma+iT}}{\sigma+iT} \sum_{\substack{\rho \\ |\gamma-T| \leq 1}} \frac{1}{\sigma+iT-\rho} \right\} d\sigma \\
 &\ll \int_{-1/4}^{\sigma_0} \frac{x^{\sigma}}{T} \{ \log A(\chi) + n_E \log T \} d\sigma \\
 &\ll \frac{x}{T \log x} \{ \log A(\chi) + n_E \log T \}. \tag{6.10}
 \end{aligned}$$

To complete our estimate we show that the first integral in (6.10) is not too large.

Lemma 6.3. Let  $\rho = \beta + i\gamma$  have  $0 < \beta < 1$ ,  $\gamma \neq t$ . If  $|t| \geq 2$ ,  $x \geq 2$ , and  $1 < \sigma_1 \leq 3$ , then

$$\int_{-1/4}^{\sigma_1} \frac{x^{\sigma+it}}{(\sigma+it)(\sigma+it-\rho)} d\sigma \ll |t|^{-1} x^{\sigma_1} (\sigma_1 - \beta)^{-1}.$$

Proof Suppose first that  $\gamma > t$ . Let  $B$  be the rectangle with vertices at  $\sigma_1 + i(t-1)$ ,  $\sigma_1 + it$ ,  $-\frac{1}{4} + it$ ,  $-\frac{1}{4} + i(t-1)$ , oriented counterclockwise. By Cauchy's

theorem,

$$\int_B \frac{x^s}{s(s-\rho)} ds = 0$$

since the integrand has no singularities inside the contour.

However, on the three sides of the rectangle other than the segment from  $-1/4 + it$  to  $\sigma_1 + it$ , the integrand is

majorized by

$$\frac{x^{\sigma_1}}{(|t| - 1)(\sigma_1 - \beta)}$$

which proves the result for  $\gamma > t$ . A similar proof for

$\gamma < t$  uses the rectangle with vertices at  $\sigma_0 + i(t+1)$ ,

$\sigma_0 + it$ ,  $-1/4 + it$ ,  $-1/4 + i(t+1)$ .

The above lemma shows that

$$\begin{aligned} \frac{1}{2\pi i} \int_{-1/4}^{\sigma_0} \frac{x^{\sigma-iT}}{\sigma-iT} \left( \sum_{\substack{\rho \\ |\gamma+T| \leq 1}} \frac{1}{\sigma+iT-\rho} \right) d\sigma &\ll \frac{x^{\sigma_0}}{T} (\sigma_0 - 1)^{-1} n_{\chi}(-T) \\ &\ll \frac{x \log x}{T} (\log A(\chi) + n_E \log T) \end{aligned} \quad (6.11)$$

for  $x \geq 2$ ,  $T \geq 2$ , and the same estimate holds for the integral involving zeroes  $\rho$  with  $|\gamma - T| \leq 1$ . [Note that if we assume the GRH for  $L(s, \chi)$ , then we can delete the  $\log x$



term in (6.11). Also, even without the GRH we could replace  $\log x$  by  $\log \log x$  by improving Lemma 6.3.]

Therefore we finally obtain

$$H_{\chi}^*(x, T) \ll \frac{x \log x}{T} (\log A(\chi) + n_E \log T). \quad (6.12)$$

If we now combine (6.8), (6.9), and (6.12), we obtain the main result of this section, namely that

$$\begin{aligned} I_{\chi}(x, T) - I_{\chi}(x, T, U) &= -V_{\chi}(x, T, U) - H_{\chi}(x, T, U) - H_{\chi}^*(x, T) \\ &\ll \frac{x \log x}{T} \{\log A(\chi) + n_E \log T\} \\ &\quad + \frac{T x^{-U}}{U} \{\log A(\chi) + n_E \log(T+U)\}. \end{aligned} \quad (6.13)$$

## §7. The explicit formula

In this section we combine the results of preceding sections in order to obtain an explicit formula for  $\psi_C(x)$  in terms of the zeroes  $\rho$ .

We first evaluate the integral  $I_{\chi}(x, T, U)$ , which was defined by (6.2). We recall that  $x \geq 2$ ,  $U = j + 1/2$  for some non-negative integer  $j$ , and  $T \geq 2$  does not equal the ordinate of any zero of any of the  $L(s, \chi)$ . By Cauchy's theorem  $I_{\chi}(x, T, U)$  equals the sum of the residues of the

integrand at poles inside  $B_{T,U}$ . Now if  $\chi = \chi_1$ , the principal character, then  $L'/L$  has a first order pole of residue  $-1$  at  $s = 1$ , and hence (this term being absent if  $\chi \neq \chi_1$ ) we obtain a contribution of

$$- \delta(\chi)x$$

from the possible pole at  $s = 1$ . Further,  $L'/L$  has a first order pole with residue  $+1$  at each nontrivial zero  $\rho$  of  $L(s, \chi)$  (the  $\rho$ 's are counted according to their multiplicity), and so such  $\rho$ 's contribute

$$\sum_{\rho} \frac{x^{\rho}}{\rho}.$$

In addition,  $L'/L$  has first order poles at the so-called trivial zeroes, which are real and nonpositive. In fact, (6.7) shows that  $L'/L$  has first order poles at  $s = -(2m-1)$ ,  $m = 1, 2, \dots$ , where the residue is  $b(\chi)$ , and first order poles at  $s = -2m$ ,  $m = 0, 1, 2, \dots$ , where the residue is  $a(\chi)$ . Hence the residues at points  $s$  with  $\text{Re}(s) < 0$  contribute

$$- b(\chi) \sum_{m=1}^{\lfloor \frac{U+1}{2} \rfloor} \frac{x^{-(2m-1)}}{2m-1} - a(\chi) \sum_{m=1}^{\lfloor U/2 \rfloor} \frac{x^{-2m}}{2m}.$$

The only remaining residue is that at  $s = 0$ , where we have

the complication that both  $x^s/s$  and  $L'/L$  may have first order poles. The Laurent series expansions show that there exist functions  $h_1(s)$  and  $h_2(s)$  which are analytic at  $s = 0$  [ $h_2(s)$  depends on  $\chi$ ], such that

$$\frac{x^s}{s} = \frac{1}{s} + \log x + sh_1(s),$$

and [using (5.9)]

$$\frac{L'}{L}(s, \chi) = \frac{a(\chi) - \delta(\chi)}{s} + r(\chi) + sh_2(s),$$

where

$$\begin{aligned} r(\chi) = & B(\chi) - \frac{1}{2} \log A(\chi) + \frac{n_E}{2} \log \pi + \delta(\chi) \\ & - \frac{b(\chi)}{2} \frac{\Gamma'}{\Gamma}\left(\frac{1}{2}\right) - \frac{a(\chi)}{2} \frac{\Gamma'}{\Gamma}(1). \end{aligned} \quad (7.1)$$

Hence the residue at  $s = 0$  is

$$r(\chi) + (a(\chi) - \delta(\chi)) \log x.$$

If we now collect all these residue terms, we find that

$$\begin{aligned} I_{\chi}(x, T, U) = & -\delta(\chi)x + \sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^{\rho}}{\rho} - b(\chi) \sum_{m=1}^{\left[\frac{U+1}{2}\right]} \frac{x^{1-2m}}{2m-1} \\ & - a(\chi) \sum_{m=1}^{\left[\frac{U}{2}\right]} \frac{x^{-2m}}{2m} + r(\chi) + (a(\chi) - \delta(\chi)) \log x. \end{aligned} \quad (7.2)$$

We now let  $U \rightarrow \infty$ . Then (7.2) and (6.13) give us the explicit formula

$$I_{\chi}(x, T) + \delta(\chi)x - \sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^{\rho}}{\rho} - r(\chi) - (a(\chi) - \delta(\chi)) \log x \\ - \frac{n_E}{2} \log(1-x^{-1}) + \frac{1}{2}(b(\chi) - a(\chi)) \log(1+x^{-1})$$

$$\ll \frac{x \log x}{T} \{ \log A(\chi) + n_E \log T \}, \quad (7.3)$$

valid for all  $x \geq 2$  and all  $T \geq 2$  which do not coincide with the ordinate of a zero. If we now let  $T \rightarrow \infty$ , (7.3) would give us an explicit formula for the inverse Mellin transform

$$\frac{1}{2\pi i} \int_{\sigma_0 - i\infty}^{\sigma_0 + i\infty} \frac{x^s}{s} \frac{L'}{L}(s, \chi) ds$$

with no error term. However, for our purposes a cruder version of (7.3) will be more useful.

Theorem 7.1. If  $x \geq 2$  and  $T \geq 2$ , then

$$\begin{aligned}
 \psi_C(x) - \frac{|C|}{|G|} x + S(x, T) \\
 \ll \frac{|C|}{|G|} \left\{ \frac{x \log x + T}{T} \log d_L + n_L \log x + \frac{n_L x \log x \log T}{T} \right\} \\
 + \log x \log d_L + n_K x T^{-1} (\log x)^2, \quad (7.4)
 \end{aligned}$$

where

$$S(x, T) = \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left\{ \sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \right\}. \quad (7.5)$$

[The inner sums in (7.5) are over the nontrivial zeroes  $\rho$  of  $L(s, \chi)$ .]

Proof Lemma 5.5 and (5.4) show that

$$r(\chi) - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \ll \log A(\chi) + n_E,$$

and so

$$\begin{aligned}
 I_\chi(x, T) + \delta(\chi)x - \sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \\
 \ll \log A(\chi) + n_E \log x + \frac{x \log x}{T} \{\log A(\chi) + n_E \log T\}.
 \end{aligned}$$

Hence by (5.1) and (6.1) we have for  $x \geq 2$ ,  $T \geq 2$  [T not

coinciding with the ordinate of any zero  $\rho$  of any  $L(s, \chi)$

$$I_C(x, T) - \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \left\{ \delta(\chi)x - \sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \right\}$$

$$\ll \frac{|C|}{|G|} \sum_{\chi} \left\{ \frac{x \log x + T}{T} \log A(\chi) + n_E \log x + \frac{n_E x \log x \log T}{T} \right\}$$

$$\ll \frac{|C|}{|G|} \left\{ \frac{x \log x + T}{T} \log d_L + n_L \log x + \frac{n_L x \log x \log T}{T} \right\}$$

since

$$\sum_{\chi} \log A(\chi) = \log d_L$$

by the conductor-discriminant formula, and  $n_E \cdot [L:E] = n_L$ .

Since  $\psi_C(x) = I_C(x, T) + R_1(x, T)$ , where  $R_1(x, T)$  satisfies

(3.18), we obtain the bound of the theorem, provided  $T$

does not equal the ordinate  $\gamma$  of some zero  $\rho = \beta + i\gamma$ . If,

however,  $T = \gamma$  for some  $\rho$ , then we evaluate (7.4) with

$T$  replaced by  $T + \varepsilon$  for a very small  $\varepsilon$ , and let  $\varepsilon \rightarrow 0$ .

The possible discontinuity in the function on the left side

comes from zeroes  $\rho$  with  $T = \gamma$ , and since there are

$\ll \sum_{\chi} n_{\chi}(T)$  of them, their contribution can be absorbed in the error term by increasing the constant implied by the  $\ll$  notation.

The above theorem, which is the main result of this paper, serves to exhibit  $\psi_C(x)$  as consisting of the main term  $\frac{|C|}{|G|} x$ , of  $S(x, T)$ , and of a relatively small remainder. In the rest of this paper we will be concerned with estimating  $S(x, T)$ . If we assume the GRH, then a good bound for  $S(x, T)$  can be easily given with what we already know. In order to obtain an unconditional result, however, we need to show that the zeroes  $\rho$  do not approach close to the line  $\operatorname{Re}(s) = 1$ .

## §8. Zero-free regions

In this section we use the classical method to prove a zero-free region for  $\zeta_L(s)$ . Since

$$\zeta_L(s) = \prod_{\chi} L(s, \chi) \quad (8.1)$$

and the  $L(s, \chi)$  are all analytic for  $s \neq 1$ , any zero-free region for  $\zeta_L(s)$  immediately implies one for each of the  $L(s, \chi)$ . This approach does have the serious disadvantage that one can often obtain larger zero-free regions by working directly with the  $L(s, \chi)$  (cf. [2; Ch. 14]); in fact, one can essentially replace  $\log d_L$  by  $\max(\log A(\chi))$  and  $n_L$  by  $n_E$  in the estimates below. The problem with that



result is that in general  $n_E$  can be almost as large as  $n_L$  and  $\max(\log A(\chi))$  almost as large as  $d_L$ . Finally, we should mention that for a fixed  $L$  a better zero-free region can be obtained by more sophisticated methods [12], but the published versions are not explicit as to the dependence on the field  $L$ .

Lemma 8.1. There is an absolute, effectively computable positive constant  $c_8$  such that  $\zeta_L(s)$  has no zeroes  $\rho = \beta + i\gamma$  in the region

$$|\gamma| \geq (1 + 4 \log d_L)^{-1}$$

$$\beta \geq 1 - c_8 (\log d_L + n_L \log(|\gamma| + 2))^{-1}.$$

Proof We have

$$-\frac{\zeta'_L}{\zeta_L}(s) = \sum_{m=1}^{\infty} \alpha(m) m^{-s} \quad (8.2)$$

for  $\sigma = \operatorname{Re}(s) > 1$ , where  $\alpha(m) \geq 0$  for all  $m$ . Hence

$$\begin{aligned} & \operatorname{Re} \left( -3 \frac{\zeta'_L}{\zeta_L}(\sigma) - 4 \frac{\zeta'_L}{\zeta_L}(\sigma + it) - \frac{\zeta'_L}{\zeta_L}(\sigma + 2it) \right) \\ &= \sum_{m=1}^{\infty} \alpha(m) m^{-\sigma} (3 + 4 \cos(t \log m) + \cos(2t \log m)) \geq 0 \end{aligned}$$

by the classical identity

$$3 + 4 \cos \theta + \cos 2\theta = 2(1 + \cos \theta)^2 \geq 0.$$

If we now consider the trivial normal extension  $L$  of  $L$ , then  $\zeta_L(s)$  is the Artin  $L$ -function associated to the principal character, and if  $\gamma_L(s)$  denotes the associated gamma factor then (5.11) shows that

$$2 \frac{\zeta'_L}{\zeta_L}(s) = \sum_{\rho} \left( \frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}} \right) - \log d_L - \frac{2}{s} - \frac{2}{s-1} - 2 \frac{\gamma'_L}{\gamma_L}(s), \quad (8.3)$$

where the summation is over the nontrivial zeroes  $\rho$  of  $\zeta_L(s)$ . We note here that if  $\operatorname{Re} s > 1$ , then  $\operatorname{Re}(s-\rho)^{-1} > 0$  for each zero  $\rho$ . If  $\rho = \beta + i\gamma$  is some particular zero with  $|\gamma| \geq (1+4 \log d_L)^{-1}$ , then we find that for  $\sigma > 1$ ,

$$\begin{aligned} - \frac{\zeta'_L}{\zeta_L}(\sigma) &\leq \frac{1}{\sigma-1} + \frac{1}{\sigma} + \frac{1}{2} \log d_L + \frac{\gamma'_L}{\gamma_L}(\sigma) - \sum_{\rho} \operatorname{Re}(\sigma-\rho)^{-1} \\ &\leq \frac{1}{\sigma-1} + c_9 \log d_L + c_9 n_L, \end{aligned}$$

$$\begin{aligned} - \operatorname{Re} \frac{\zeta'_L}{\zeta_L}(\sigma+2i\gamma) &\leq \frac{1}{2} \log d_L + \operatorname{Re} \left\{ \frac{1}{\sigma+2i\gamma-1} + \frac{1}{\sigma+2i\gamma} \right\} \\ &\quad + \operatorname{Re} \frac{\gamma'_L}{\gamma_L}(\sigma+2i\gamma) \end{aligned}$$

$$\leq c_{10} \log d_L + c_{10} n_L \log(|\gamma| + 2),$$

and

$$- \operatorname{Re} \frac{\zeta'_L}{\zeta_L}(\sigma + i\gamma) \leq c_{11} \log d_L + c_{11} n_L \log(|\gamma| + 2) - \frac{1}{\sigma - \beta},$$

where in the last inequality we have included the contribution of the zero  $\rho = \beta + i\gamma$ . These inequalities and (8.2) show that for all  $\sigma > 1$ ,

$$\frac{4}{\sigma - \beta} < \frac{3}{\sigma - 1} + c_{12} \{\log d_L + n_L \log(|\gamma| + 2)\}.$$

If we now set  $\sigma = 1 + (100c_{12})^{-1} \{\log d_L + n_L \log(|\gamma| + 2)\}^{-1}$ , say, then we obtain the result of the lemma.

In addition to Lemma 8.1 we also need information about zeroes of  $\zeta_L(s)$  very near the real axis. Such information can be obtained by methods similar to those used above.

**Lemma 8.2.** If  $n_L > 1$  then  $\zeta_L(s)$  has at most one zero  $\rho = \beta + i\gamma$  in the region

$$|\gamma| \leq (4 \log d_L)^{-1}, \tag{8.4}$$

$$\beta \geq 1 - (4 \log d_L)^{-1}.$$

This zero, if it exists, has to be real and simple.

**Proof** Identity (8.3) shows that for  $1 < \sigma \leq 2$ ,

$$\sum_{\rho} \frac{\sigma - \beta}{(\sigma - \beta)^2 + \gamma^2} = \frac{1}{\sigma - 1} + \frac{1}{2} \log d_L + \frac{\zeta'_L}{\zeta_L}(\sigma) + \frac{1}{\sigma} + \frac{\gamma'_L}{\gamma_L}(\sigma)$$

$$\leq \frac{1}{\sigma - 1} + \frac{1}{2} \log d_L \quad (8.5)$$

since  $\zeta'/\zeta \leq 0$  and it is easily verified that

$$\frac{1}{\sigma} + \frac{\gamma'_L}{\gamma_L}(\sigma) = \left(\frac{1}{\sigma} - \frac{n_L}{2} \log \pi\right) + \frac{a(L)}{2} \frac{\Gamma'}{\Gamma}\left(\frac{\sigma}{2}\right)$$

$$+ \frac{b(L)}{2} \frac{\Gamma'}{\Gamma}\left(\frac{\sigma+1}{2}\right) < 0$$

for  $1 < \sigma \leq 1 + (\log 3)^{-1}$ . If  $\rho = \beta + i\gamma$  is in the region described by (8.4) and  $\gamma \neq 0$ , then (8.5) gives

$$2 \frac{\sigma - \beta}{(\sigma - \beta)^2 + \gamma^2} \leq \frac{1}{\sigma - 1} + \frac{1}{2} \log d_L,$$

which is false at  $\sigma = 1 + (\log d_L)^{-1} \leq 1 + (\log 3)^{-1}$ . We similarly obtain a contradiction if there is more than one real zero in our region.

If the possible zero described by the above lemma exists, we denote it by  $\beta_0$  and call it the exceptional (Siegel) zero. We also note that if  $n_L = 1$  (so that  $L = \mathbb{Q}$ ,  $\log d_L = 0$ ), then  $\zeta_L$  has no nontrivial zeroes  $\rho$  with  $|\gamma| < 14$ . If  $\beta_0$  exists, then (8.1) shows that there exists

a unique  $\chi_0$  such that  $L(\beta_0, \chi_0) = 0$ . This  $\chi_0$  must then be a real character, as  $L(\beta_0, \bar{\chi}_0) = \overline{L(\beta_0, \chi_0)} = 0$ .

### §9. Final estimates

We conclude this paper by applying the explicit formula of Theorem 7.1 to estimate  $\psi_C(x)$  and  $\pi_C(x)$ . We start with the GRH estimate for  $\psi_C(x)$ , which is the easiest to obtain.

Theorem 9.1 If  $\zeta_L(s)$  satisfies the GRH, then

$$\psi_C(x) - \frac{|C|}{|G|} x \ll \frac{|C|}{|G|} x^{\frac{1}{2}} \log x \log d_L x^{n_L} + \log x \log d_L \quad (9.1)$$

for all  $x \geq 2$ .

Proof If  $\zeta_L(s)$  satisfies the GRH, then so do all of the  $L(s, \chi)$ . Therefore, for each  $\chi$  there are no nontrivial zeroes  $\rho$  with  $|\rho| < 1/2$ , and so by Lemma 5.4.

$$\begin{aligned} \left| \sum_{\substack{\rho \\ |\gamma| < T}} \frac{x^\rho}{\rho} + \sum_{|\rho| < \frac{1}{2}} \frac{1}{\rho} \right| &\leq x^{\frac{1}{2}} \sum_{\substack{\rho \\ |\gamma| < T}} \frac{1}{|\rho|} \\ &\ll x^{\frac{1}{2}} \sum_{j=1}^{[T]} \frac{n_x(j)}{j} \\ &\ll x^{\frac{1}{2}} \{ \log A(\chi) + n_E \log T \} \log T, \end{aligned}$$

which together with (7.5) implies

$$S(x, T) \ll \frac{|C|}{|G|} x^{\frac{1}{2}} \{\log d_L + n_L \log T\} \log T \quad (9.2)$$

for all  $T \geq 2$ . We now choose  $T = x^{\frac{1}{2}} + 1$ , say, and then (9.2) and (7.4) imply (9.1) for  $x \geq 2$ .

Theorem 9.2. There is an effectively computable positive absolute constant  $c_{13}$  such that if

$$x \geq \exp(4n_L (\log d_L)^2) \quad (9.3)$$

then

$$\psi_C(x) = \frac{|C|}{|G|} x - \frac{|C|}{|G|} \chi_0(g) \frac{x^{\beta_0}}{\beta_0} + R(x), \quad (9.4)$$

where

$$|R(x)| \leq x \exp(-c_{13} n_L^{-\frac{1}{2}} (\log x)^{\frac{1}{2}}),$$

and where the second term on the right side of (9.4) occurs only if  $\zeta_L(s)$  has an exceptional zero  $\beta_0$ , and  $\chi_0$  is the (real) character of  $H = \text{Gal}(L/E) = \langle g \rangle$  for which  $L(s, \chi_0, L/E)$  has  $\beta_0$  as a zero.

Proof If  $\rho = \beta + i\gamma \neq \beta_0$  is a nontrivial zero of one of the  $L(s, \chi)$  with  $|\gamma| \leq T$ , then the unconditional bound of

Lemma 8.1 shows that

$$|x^\rho| = x^\beta \leq x \exp(-c_{14} \frac{\log x}{\log d_L T^{n_L}})$$

for  $x \geq 2$ ,  $T \geq 2$ . Further, Lemma 5.4 shows that

$$\sum_x \sum_{\substack{\rho \\ |\rho| \geq \frac{1}{2} \\ |\gamma| \leq T}} \left| \frac{1}{\rho} \right| \ll \log T \log(d_L T^{n_L}).$$

Also,

$$\sum_x \sum_{\substack{\rho \neq 1-\beta_0 \\ |\rho| < \frac{1}{2}}} \left\{ \left| \frac{x^\rho}{\rho} \right| + \left| \frac{1}{\rho} \right| \right\} \ll x^{\frac{1}{2}} \sum_x \sum_{\substack{\rho \neq 1-\beta_0 \\ |\rho| < \frac{1}{2}}} \left| \frac{1}{\rho} \right| \ll x^{\frac{1}{2}} (\log d_L)^2,$$

by Lemma 5.4 and the fact that for  $\rho \neq 1 - \beta_0$ ,

$|\rho| \geq (4 \log d_L)^{-1}$ . (If  $\log d_L = 0$ ,  $L = \mathbb{Q}$ , and the

estimate holds trivially). Finally,

$$\frac{x^{1-\beta_0}}{1-\beta_0} - \frac{1}{1-\beta_0} = x^\sigma \log x \leq x^{\frac{1}{2}} \log x$$

for some  $\sigma$ ,  $0 \leq \sigma \leq 1 - \beta_0$ . Collecting all these

estimates gives us



$$\begin{aligned}
 S(x, T) &= \frac{|C|}{|G|} \chi_0(g) \frac{x^{\beta_0}}{\beta_0} \\
 &\ll \frac{|C|}{|G|} x \log T \log(d_L T^{n_L}) \exp\left(-\frac{c_{14} \log x}{\log d_L T^{n_L}}\right) \\
 &\quad + \frac{|C|}{|G|} x^{\frac{1}{2}} (\log d_L)^2. \tag{9.5}
 \end{aligned}$$

We now choose

$$T = \exp(n_L^{-\frac{1}{2}} (\log x)^{\frac{1}{2}} - \log d_L). \tag{9.6}$$

The estimate of the theorem then follows from (9.5) and (7.4).

The deduction of Theorems 1.1 and 1.3 from the preceding theorems is now straightforward. We first define the function

$$\begin{aligned}
 \theta_C(x) &= \sum_{\substack{P \text{ unramified} \\ N_{K/Q} P \leq x \\ [\frac{L/K}{P}] = C}} \log(N_{K/Q} P).
 \end{aligned}$$

Since there are at most  $n_K$  ideals  $P^m$  ( $P$  prime) of a given norm in  $K$ ,

$$\sum_{\substack{P, m \\ m \geq 2 \\ N_{K/Q} P^m \leq x}} \log(N_{K/Q} P) \ll n_K x^{\frac{1}{2}} \quad (9.7)$$

by an elementary Chebyshev-type estimate. This shows that the estimates of Theorems 9.1 and 9.2 hold when  $\psi_C(x)$  is replaced by  $\theta_C(x)$ . Theorems 1.1 and 1.3 now follow from these estimates for  $\theta_C(x)$  by simple partial summation arguments.

We conclude this paper by indicating one way in which the GRH estimate of Corollary 1.2 can be slightly improved. Instead of integrating

$$\frac{1}{2\pi i} \int \frac{x^s}{s} F_C(x) ds,$$

we can integrate

$$\frac{1}{2\pi i} \int \left( \frac{y^{s-1} - x^{s-1}}{s-1} \right)^2 F_C(x) ds,$$

where  $y > x > 1$ , along the contour  $B_{T,U}$  of Section 6. We then first let  $U \rightarrow \infty$ , and then  $T \rightarrow \infty$ . The integral from  $\sigma_0 - i\infty$  to  $\sigma_0 + i\infty$  gives us the term we are interested in, i.e.,

$$\sum_P \frac{\log NP}{NP} r(NP; y, x), \quad (9.8)$$

$$\left[ \frac{L/K}{P} \right] = C$$

where

$$r(m; y, x) = \begin{cases} \log \frac{m}{x^2} & x^2 \leq m \leq xy, \\ \log \frac{y^2}{m} & xy \leq m \leq y^2, \\ 0 & \text{otherwise,} \end{cases}$$

together with the contribution of the ramified primes and prime powers. By Cauchy's theorem the value of the integral also equals the contribution of the poles of the integrand, which is

$$\frac{|C|}{|G|} \left( \log \frac{y}{x} \right)^2 - \frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) \sum_{\rho} \left( \frac{y^{\rho-1} - x^{\rho-1}}{\rho-1} \right)^2, \quad (9.9)$$

where  $\rho$  now runs through both the trivial and the nontrivial zeroes of  $L(s, \chi)$ . If we now choose  $x = \log d_L$ ,  $y = c_{14} x$ , then for  $c_{14}$  sufficiently large (and on the assumption of the GRH) the main term in (9.9) will dominate both the sum over the zeroes and of the ramified prime and prime power factors, so that (9.8) will have to be nonzero. Hence there will be a prime  $P$  with  $\left[ \frac{L/K}{P} \right] = C$  and

$$NP \leq y^2 \leq c_{14}^2 \log^2 d_L.$$

## REFERENCES

1. E. Bombieri, Le grand crible dans la théorie analytique des nombres, Soc. math. France, Astérisque, 18, 1974.
2. H. Davenport, Multiplicative Number Theory, Markham, Chicago, 1967, MR 36 #117.
3. M. Deuring, Über den Tschebotareffschen Dichtigkeitssatz, Math. Ann., 110 (1934), 414-415.
4. E. Fogels, On the zeroes of Hecke's L-functions. I, II, III, Acta Arith., 7 (1961), 87-106; 7 (1961), 131-147; 8 (1963), 307-309. MR 25 # 55, 28 #67.
5. L.J. Goldstein, A generalization of the Siegel-Walfisz theorem, Trans. Am. Math. Soc., 149 (1970), 417-429. MR 43 #181.
6. H. Heilbronn, Zeta-functions and L-functions, pp. 204-230 in Algebraic Number Theory, J.W.S. Cassels and A. Fröhlich, eds., Academic Press, 1967.
7. J.C. Lagarias, H.L. Montgomery, and A.M. Odlyzko, An upper bound for the least prime ideal in the Chebotarev density theorem, to be published.
8. S. Lang. On the zeta function of number fields, Inventiones math., 12 (1971), 337-345.
9. C.R. MacCluer, A reduction of the Cebotarev density theorem to the cyclic case, Acta Arith., 15 (1968), 45-47. MR 38 # 2117.
10. C.J. Moreno, An effective Chebotarev density theorem, to be published.
11. A.M. Odlyzko, On conductors and discriminants, Durham Symposium.

12. A.V. Sokolovskii, A theorem on the zeros of Dedekind's zeta function and the distance between "neighboring" prime ideals (Russian), *Acta Arith.* 13 (1967/68), 321-334. MR 36 ~~#~~6380.
13. H.M. Stark, Some effective cases of the Brauer-Siegel theorem, *Inventiones math.*, 23 (1974), 135-152.
14. E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford 1951. MR 13 ~~#~~174.
15. N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math. Ann.*, 95 (1926), 191-228.
16. B.L. van der Waerden, *Modern Algebra*, 3rd ed., Ungar, New York, 1950.
17. E.T. Whittaker and G.N. Watson, *A Course of Modern Analysis*, 4th ed., Cambridge Univ. Press, 1965.

## Odlyzko bounds and class number problems

John Masley

In this expository article we indicate how the bounds of Odlyzko ([10-12]) and Galois actions combine to give information about ideal class groups. In particular, small class number problems can be solved.

In §1 we recall some results of Odlyzko and show how they yield a bound on the class numbers of some fields. In §2 we list some algebraic theorems which are useful in obtaining information on the order and structure of ideal class groups. In §3 we give a sketch of the proof that only 29 proper extensions of the rational field  $\mathbb{Q}$  are full cyclotomic fields with (wide) class number one. The 29 fields are all full cyclotomic fields of degree  $< 21$  plus the fields of degree 24 corresponding to  $35^{\text{th}}$ ,  $45^{\text{th}}$ , and  $84^{\text{th}}$  roots of unity.

By a number field  $K$  we shall always mean a finite extension of  $\mathbb{Q}$ . The ideal class group of  $K$  is fractional

ideals of  $K$  modulo all principal ideals and will be denoted  $P_K$ . The cardinality of  $P_K$  is the class number of  $K$  and will be denoted by  $h_K$ .

We shall use  $\mathbb{C}_m$  to denote the field  $\mathbb{Q}(\exp 2\pi i/m)$  and  $\mathbb{C}_m^+$  to denote its maximal real subfield  $\mathbb{Q}(\cos 2\pi/m)$ . We abbreviate  $h_{\mathbb{C}_m}$  to  $h_m$  and  $h_{\mathbb{C}_m^+}$  to  $h_m^+$ . Then  $h_m = h_m^* h_m^+$  where  $h_m^*$  is an integer called the relative class number for  $\mathbb{C}_m$ . Since  $\mathbb{C}_m = \mathbb{C}_{2m}$  for  $m$  odd we shall always assume for simplicity that  $m \not\equiv 2 \pmod{4}$ .

### §1. The analytic theory

In a series of recent articles, Andrew Odlyzko has shown how to derive lower bounds for the absolute value of the discriminant of a number field  $K$  which depend only on  $|K:\mathbb{Q}|$  and the number of real embeddings of  $K$  (i.e.  $r_1(K)$ ). His results may be stated as follows:

Theorem (Odlyzko) Let  $K$  be an algebraic number field with discriminant  $d_K$ , degree  $n$ , and  $r_1$  real embeddings. Put

$a = r_1/n$  and let  $G(s) = -\frac{1+a}{2} \frac{\Gamma'}{\Gamma}(\frac{s}{2}) + \frac{a-1}{2} \frac{\Gamma'}{\Gamma}(\frac{s+1}{2})$ . Then

$$(1) \quad |^n \sqrt{d_K}| > (60.1)^a (22.2)^{1-a} e^{-\frac{254}{n}}$$



$$(2) \quad |^n\sqrt{d_K}| > (58.6)^a (21.8)^{1-a} e^{-\frac{70}{n}}$$

$$(3) \quad \log |^n\sqrt{d_K}| > \log \pi + G(\sigma) - \left(\sigma - \frac{1}{2}\right) G'(\tilde{\sigma}) - \frac{2}{\sigma-1} - \frac{2}{\sigma} \\ - \left(\sigma - \frac{1}{2}\right) \left\{ \frac{2}{(\tilde{\sigma}-1)^2} + \frac{2}{\tilde{\sigma}^2} \right\}$$

where  $\sigma, \tilde{\sigma}$  are any real numbers with  $\sigma > 1$ ,

$$\tilde{\sigma} \geq \text{Max}(1 + .28108\sigma, \frac{5 + \sqrt{12\sigma^2 - 5}}{6}).$$

In the sequel we shall call  $|^n\sqrt{d_K}|$  the root-discriminant of  $K$  and denote it  $rd_K$ . The root-discriminants of  $\mathbb{C}_m$  and  $\mathbb{C}_m^+$  will be denoted by  $rd_m$  and  $rd_m^+$  respectively.

The connection between root-discriminants and class numbers depends on the following:

Lemma Let  $E/F$  be an extension of number fields unramified at all finite primes. Then  $rd_E = rd_F$ . In particular, the Hilbert class field of a number field has the same root-discriminant as the number field.

Proof We have  $|d_E| = |d_F|^{[E:F]}$  since the relative discriminant ideal for  $E/F$  is the ring of integers in  $F$ .

The result follows upon taking  $|E:\mathbb{Q}|$ -th roots.

Let  $a \in \mathbb{Q}$ ,  $0 \leq a \leq 1$ . Call a number field of type  $a$  if  $r_1(K)|K:\mathbb{Q}|^{-1} = a$ . Let  $A$  be the set of positive multiples of the order of the image of  $a$  in  $\mathbb{Q}/\mathbb{Z}$ . Call an increasing function  $f_a: A \rightarrow \{x \in \mathbb{R} \mid x > 0\}$  a class number bound function of type  $a$  if for all  $x \in A$  we have  $f_a(x) < \inf rd_K$  where the  $\inf$  is taken over all number fields of type  $a$  and degree  $x$ . Then we obtain the

Theorem (Class number bound). Let  $K$  be a number field of type  $a$  and let  $f_a$  be a class number bound function of type  $a$ . Then  $f_a(x) > rd_K$  implies  $h_K < x|K:\mathbb{Q}|^{-1}$ .

Proof. If  $K$  is of type  $a$ , then its Hilbert class field  $H_K$  is also of type  $a$  since every real infinite prime of  $K$  splits into  $h_K$  real infinite primes of  $H_K$  and this accounts for all the real infinite primes of  $H_K$ . By the Lemma  $rd_{H_K} = rd_K$  so  $f_a(x) > rd_K = rd_{H_K} > f_a(|H_K:\mathbb{Q}|) = f_a(h_K|K:\mathbb{Q}|)$ . Since  $f_a$  is increasing we're done.

Odlyzko's Theorem allows one to construct a class number

bound function of type a. There is a table at the end of [12] which gives some values of a class number bound function of type 0 (for totally complex fields) and of type 1 (for totally real fields).

Example: Let  $f_1$  be the class number bound function for totally real fields constructed from Odlyzko's tables [12] (extended to large positive integers via inequalities (1) and (2)). Then  $f_1(24) > 18 > 2 \cdot 11 \cdot 9 = \text{rd}_{44}^+$ . Since  $|\mathfrak{c}_{44}^+ : \mathbb{Q}| = 10$ ,  $h_{44}^+ \leq 2$ . In a similar fashion, one finds for all  $m$  with  $|\mathfrak{c}_m^+ : \mathbb{Q}| \leq 12$  that  $h_m^+ \leq 2$ . In fact, for these values of  $m$ , one finds  $h_m^+ = 1$  except possibly for  $m = 32, 44, 23, 52, 56$ , and  $72$ .

## §2. The algebraic theory

In this section we list some theorems which give useful information about ideal class groups. Here  $p$  will always denote a prime number.

Rank Theorem Let  $E/F$  be a cyclic extension of degree  $n$  and suppose  $p$  is a prime which divides neither  $n$  nor  $h_E$ , for all  $E'$  with  $E \not\subseteq E' \subseteq F$ . Then the  $p$ -rank of  $P_E$  is either 0 or

at least  $f = \text{the order of } p \bmod n$ . In particular,  $p | h_E$  implies  $p^f | h_E$ .

The proof of this theorem will appear in a forthcoming paper of the author. A similar theorem is proved in Frohlich [2] and Iwasawa [5]. The key fact is that if  $P_E$  has non-trivial  $p$ -primary component,  $\text{Gal}(E/F)$  acts non-trivially on this component. Iwasawa's result is sufficient for the following:

Example. By the methods of §1 we see that  $h_{59}^+ < 29 = |c_{59}^+ : \mathbb{Q}|$ . But if any  $p < 29$  divides  $h_{59}^+$  then  $p^f$ , a number congruent to 1 mod 29, must divide  $h_{59}^+$  which violates the bound. Hence  $h_{59}^+ = 1$ .

Pushing-down Theorem. Let  $E/F$  be a  $p$ -extension and suppose that only one prime divisor of  $F$  is ramified in  $E$  and that this prime is totally ramified. Then  $p | h_E$  implies  $p | h_F$ .

This theorem appears in [3], [4], and [14].

Example. We see that  $h_{100}^+ \leq 5$  and  $h_{20}^+ = 1$  from §1.

Since  $|\mathbb{C}_{100}^+ : \mathbb{C}_{20}^+| = 5$  and only the unique prime above 5 ramifies,  $5 \nmid h_{100}^+$ . Also, the Rank Theorem applied to  $\mathbb{C}_{100}^+/\mathbb{C}_{20}^+$  shows that  $(h_{100}^+, 6) = 1$  so  $h_{100}^+ = 1$ . We know  $h_{100}^* = 55$  so  $\mathbb{C}_{100}$  has class number 55.

(p,p) Theorem. Let  $E/F$  be an abelian extension of type  $(p,p)$ . If  $q \neq p$  is a prime divisor of  $h_E$ , then  $q$  divides the class number of one of the  $p + 1$  proper intermediate fields between  $E$  and  $F$ .

A proof of this theorem using the action of  $\text{Gal}(E/F)$  on  $p_E$  is given in [2] and [8].

Example.  $\mathbb{C}_{63}^+/\mathbb{Q}(\sqrt{21})$  is a  $(3,3)$ -extension and by §1  $h_{63}^+ \leq 3$ . The Pushing-down Theorem applied to  $\mathbb{C}_{63}^+/\mathbb{C}_{21}^+$  shows that  $3 \nmid h_{63}^+$  and if  $2 \mid h_{63}^+$  then  $K$ , one of the four cubic extensions of  $\mathbb{Q}(\sqrt{21})$  contained in  $\mathbb{C}_{63}^+$ , would have even class number. The Rank Theorem would then imply that  $4 \mid h_K$  and consequently  $4 \mid h_{63}^+$ . Hence  $h_{63}^+ = 1$  and  $h_{63} = h_{63}^* = 7$ .

### §3. The class number one problem for $\mathbb{C}_m$

In this section we sketch a solution of the class

number one problem for cyclotomic fields. Our result is:

Theorem. Let  $m > 2$  be an integer not congruent to 2 mod 4.

Then  $\mathbb{C}_m = \mathbb{Q}(\exp 2\pi i/m)$  has class number one only for  $m = 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60$ , and 84.

Proof. Since  $h_m = h_m^+ h_m^*$  we are looking for  $m$  with  $h_m^+ = h_m^* = 1$ . The following facts about  $h_m^*$  are known ([6] and [9]):

- i) If  $m|n$  then  $h_m^* | h_n^*$ .
- ii) If four primes divide  $m$  then  $4 | h_m^*$ .
- iii) For primes  $p$ ,  $h_p^* > 1$  for  $p > 19$  and  $h_{p^a}^* > 16$  for  $p^a > 32$ .

Since  $h_m^*$  is easily calculated (see [13]) we check that the 29 values of  $m$  cited in the Theorem are the only ones with relative class number  $h_m^* = 1$ . Since all of them have

$|\mathbb{C}_m^+ : \mathbb{Q}| \leq 12$ , by the example at the end of §1 we need verify only that  $h_{32}^+ \neq 2$  and that  $h_{44}^+ \neq 2$ . The Pushing-down Theorem applies to  $\mathbb{C}_{32}^+/\mathbb{Q}$  and the Rank Theorem applies to  $\mathbb{C}_{44}^+/\mathbb{Q}(\sqrt{11})$  so we are done.

Notes: (1) Previous proofs of this theorem relied on

computations in [1]. Using Odlyzko's bounds we no longer need these computations for the proof.

(2) Other small class number problems can be solved.

For example, the remaining  $m$  with  $|\mathfrak{C}_m^+ : \mathbb{Q}| \leq 12$  are the solutions to the class number two and class number three problems (cf. [7], [8]).

#### REFERENCES

1. H. Bauer, Numerische Bestimmung von Klassenzahlen reeler zyklischer Zahlkörper J. of Number Theory, 1 (1969), 161-162.
2. A. Fröhlich, On the class group of relatively Abelian fields, Quart. J. Math. Oxford (2), 3 (1952), 98-106.
3. A. Fröhlich, On a Method for the Determination of Class Number Factors in Number Fields, Mathematika, 4 (1957), 113-121.
4. K. Iwasawa, A Note on Class Numbers of Algebraic Number Fields, Abh. Math. Sem. Univ. Hamburg, 20 (1956), 257-258.
5. K. Iwasawa, A Note on Ideal Class groups, Nagoya Math J., 27 (1966), 239-247.
6. J. Masley, On the class number of cyclotomic fields, Princeton University (1972), dissertation.
7. J. Masley, Solution of the Class Number Two Problem for Cyclotomic Fields, Inventiones Math., 28 (1975), 243-244.
8. J. Masley, Solution of Small Class Number Problems for Cyclotomic Fields, to appear in Compositio Mathematica.



9. J. Masley and Hugh L. Montgomery, Cyclotomic Fields with Unique Factorization, to appear in Crelle.
10. A. Odlyzko, Some Analytic Estimates of Class Numbers and Discriminants, *Inventiones Math.*, 29 (1975), 275-286.
11. A. Odlyzko, Lower Bounds for Discriminants of Number Fields II, to appear.
12. A. Odlyzko, On Conductors and Discriminants, Durham Symposium.
13. G. Schrutka v. Rechtenstamm, Tabelle der (relativ-) Klassenzahlen von Kreiskörper, *Abh. Deutsche Akad. Wiss. Berlin*, 1964 Math. Nat. Kl. Nr. 2.
14. A. Yokoyama, On Class Numbers of Finite Algebraic Number Fields, *Tohoku Math. J.*, 17 (1965), 349-357.

A Relation Between  $\zeta_K(s)$  and  $\zeta_K(s-1)$  for any  
Algebraic Number Field  $K$

Audrey Terras

§0. Introduction

No, there is no misprint in the title. We meant  $s-1$  and not  $1-s$ . For  $\zeta_K(s)$  and  $\zeta_K(s-1)$  both appear in the constant term of the Fourier expansion of a certain non-analytic Eisenstein series for the number field  $K$ . A similar Fourier expansion is the starting point for Deligne's method of obtaining congruences between values of  $L$ -functions [7]. The difference is that our Eisenstein series are nonanalytic in the sense of Maass [4, Chapter 4]. So we do not have to assume that the number field is totally real (cf. [8, Chapter III, especially p. 233]). Another consequence of the fact that the Eisenstein series which we use are not complex analytic functions is that we find  $K$ -Bessel functions in our Fourier coefficients (cf. [4, Chapter 4, especially p. 212] or [3, §2.2]). A result

is that congruences seem out of the question.

### §1. Summary of Results

The usual litany of notation must be recited. The degree of  $K$  over  $\mathbb{Q}$  is  $m$ . Let  $x \mapsto x^{(j)}$  ( $j = 1, \dots, r_1$ ) denote the real embeddings  $K \rightarrow \mathbb{R}$  and  $x \mapsto x^{(j)} = x^{\frac{(j+r_2)}{2}}$  ( $j = r_1 + 1, \dots, r_1 + r_2$ ) denote the complex embeddings  $K \rightarrow \mathbb{C}$ . Then  $m = r_1 + 2r_2$ . We need to set  $e_j = 1$  ( $j = 1, \dots, r_1$ ) and  $e_j = 2$  ( $j = r_1 + 1, \dots, r_1 + r_2$ ). The different will be denoted by  $d_K$ , the absolute value of the discriminant by  $d_K$ , the regulator by  $R_K$ , the number of roots of unity by  $w_K$ , the class number by  $h_K$ .

As in Martinet's lectures [5] we need to define the usual combination of the Dedekind zeta function and the appropriate  $\Gamma$ -factors:

$$\Lambda_K(s) = A^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s),$$

where  $A = 2^{-r_2} \pi^{-m/2} \sqrt{d_K}$ . We shall also need the generalized divisor function of any integral ideal  $a$  of  $K$ , defined by:

$$\sigma_s(a) = \sum_{b|a} N b^s.$$

Here the sum is over integral ideals  $b$  dividing  $a$ .

Finally a rather complicated looking function must be built up out of K-Bessel functions:

$$K_s(z) = \frac{1}{2} \int_0^\infty e^{-\frac{z}{2}(t + \frac{1}{t})} t^{s-1} dt, \quad$$

for  $|\arg z| < \frac{\pi}{2}$ . First define

$$M_s(z) = K_s(z) + 2z \frac{d}{dz} K_s(z).$$

Then for  $u$  in the field  $K$ , set

$$T(s, u) = M_{\frac{e_1 s}{2}}(2\pi e_1 |u^{(1)}|) \prod_{j=1}^{r_1+r_2} K_{\frac{e_j s}{2}}(2\pi e_j |u^{(j)}|).$$

At last we can state the main result:

Theorem.  $(2-s)\Lambda_K(s-1) + s\Lambda_K(s)$

$$= -2^{\frac{r_1+r_2}{2}} d_K^{\frac{s-1}{2}} \sum_{0 \neq u \in d_K^{-1}} |Nu|^{\frac{s-1}{2}} \sigma_{1-s}(u d_K) T(s-1, u).$$

An easy consequence is:

Corollary.  $h_{K,K}^R = 2w_K (2\pi)^{-m} d_K \zeta_K(2)$

$$+ w_K 2^{\frac{r_2}{2}} d_K^{\frac{1}{2}} \sum_{0 \neq u \in d_K^{-1}} |Nu|^{\frac{1}{2}} \sigma_{-1}(u d_K) T(1, u).$$

For example, if  $K$  is a totally real field,  $K_{\frac{1}{2}}(z) = \sqrt{\frac{\pi}{2z}} e^{-z}$

implies that:

$$h_{K,K}^R = 4(2\pi)^{-m} d_K \zeta_K(2)$$

$$-2^{3-m} d_K^{1/2} \pi \sum_{0 \neq u \in d_K^{-1}} |u^{(1)}|_{\sigma_{-1}(u d_K)} \exp\{-2\pi(|u^{(1)}| + \dots + |u^{(m)}|)\}.$$

The Brauer-Siegel Theorem ([10]) then tells us that something complicated is happening with the sum over the inverse different as  $h_{K,K}^R$  should look like  $d_K^{1/2}$  rather than  $d_K$ .

Results similar to the theorem are to be found in work of Ramanujan and Grosswald [2]. It should not be too hard to extend the results to Hecke L-functions.

## §2. Fourier Expansions of Nonanalytic Eisenstein Series for $GL_2$ over $K$ .

The proof of the theorem stated in the preceeding section comes from the Fourier expansions we are about to discuss. The details are in [13]. Let us first consider the nonanalytic Eisenstein series in the ancient case  $K = \mathbb{Q}$ . Then the function under consideration is the Epstein zeta function  $Z(P, s)$  of a positive definite symmetric  $2 \times 2$  matrix  $P$  and a complex variable  $s$ . If  $\text{Re } s > 1$ , the definition is:

$$Z(P, s) = \frac{1}{2} \sum_{(m,n) \neq (0,0)} P \begin{bmatrix} m \\ n \end{bmatrix}^{-s}.$$

Here  $P \begin{bmatrix} m \\ n \end{bmatrix} = (mn)P \begin{pmatrix} m \\ n \end{pmatrix} = p_1 m^2 + 2p_{12} mn + p_2 n^2$ , if

$$P = \begin{pmatrix} p_1 & p_{12} \\ p_{12} & p_2 \end{pmatrix}.$$

We shall use  $P_2 = P_2^{\mathbb{Q}}$  to denote the symmetric space of  $2 \times 2$  positive definite symmetric matrices. This space is easily identified with  $GL_2(\mathbb{R})/O(2)$ , where the action of  $T \in GL_2(\mathbb{R})$  on  $P \in P_2$  is given by  $P \mapsto P[T] = {}^t T P T$ , with  ${}^t T$  = transpose of  $T$ . Then  $Z(P, s)$  is an automorphic form on  $P_2$  in the sense of Borel [1, p.200], where 3 properties are listed. Complex analyticity is replaced by the property of being an eigenfunction of all invariant differential operators on the symmetric space  $P_2$ . And the invariance property is:

$$Z(P[A], s) = Z(P, s),$$

for  $A \in GL_2(\mathbb{Z}) = \{A \mid A \text{ } 2 \times 2 \text{ integer entries, } \det A = \pm 1\}$ .

The last property describes behavior at  $\infty$ .

Writing what is essentially the Iwasawa decomposition for  $GL_2(\mathbb{R})$  as

$$P = \begin{pmatrix} t & 0 \\ 0 & p_2 \end{pmatrix} \left[ \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \right], \quad \text{for } P \in P_2,$$

one easily sees that the invariance property implies that  $Z(P, s)$  is a periodic function of  $q$ . Thus it makes sense to consider the Fourier expansion:

$$p_2^s \Gamma(s) Z(P, s) = \zeta(2s) \Gamma(s) + \left(\frac{t}{p_2}\right)^{1/2-s} \pi^{+\frac{1}{2}} \Gamma\left(s - \frac{1}{2}\right) \zeta(2s - 1) \\ + 4\pi^s \left(\frac{t}{p_2}\right)^{\frac{1}{4} - \frac{s}{2}} \sum_{n \geq 1} \cos(2\pi n g) \sigma_{1-2s}(n) n^{s-1/2} K_{1/2-s}\left(2\pi n \sqrt{\frac{t}{p_2}}\right).$$

This result is very old (cf. [9, p.44]). It implies (cf. [12]) the functional equation and analytic continuation of  $Z(P, s)$ , the Kronecker limit formula, the existence of an  $s_0$  in the open interval  $(0, 1)$  with  $Z(P, s_0) = 0$  provided that  $\frac{t}{p_2}$  is sufficiently large. Moreover the extension of this Fourier expansion to Epstein zeta functions with characters is central to Stark's solution of the class number one problem for imaginary quadratic fields [9].

Now that we have seen the Fourier expansion of the nonanalytic Eisenstein series for  $GL_2$  over  $\mathbb{Q}$ , what is the corresponding result over the number field  $K$ ? First define  $P_2^K$  to be the space of vectors  $P = (P_1, \dots, P_{r_1+r_2})$  whose  $1^{st}$   $r_1$  components are positive definite  $2 \times 2$



symmetric matrices and whose last  $r_2$  components are positive definite  $2 \times 2$  Hermitian matrices. We are looking only at the infinite part of an adelic object (cf. [1, pp. 113 ff.]) following Hecke. If  $O_K$  is the ring of integers of  $K$ , then  $GL_2(O_K)$  denotes the group of  $2 \times 2$  matrices  $A$  with entries in  $O_K$  and determinant in  $U_K =$  units of  $O_K$ . The action of  $A \in GL_2(O_K)$  on  $P \in P_2^K$  is given by  $P \mapsto P\{A\}$ , with

$$(P\{A\})_j = \overline{t_A^{(j)}} P_j A^{(j)} \quad (j = 1, \dots, r_1 + r_2).$$

Here  $A^{(j)}$  denotes the matrix obtained from  $A$  by conjugating all entries. There exists a reduction theory for  $P_2^K$  modulo  $GL_2(O_K)$  generalizing Minkowski's for  $K = \mathbb{Q}$  (cf. Borel [1, pp. 20 ff.] and Weyl [14]).

The Epstein zeta function alias the Eisenstein series over  $K$  is defined for an integral ideal  $\mathfrak{a}$  of  $K$  by:

$$Z^{\mathfrak{a}}(P, s) = \sum_{0 \neq g \in \mathfrak{a}^2 / U_K} \prod_{j=1}^{r_1+r_2} P^{(j)} \{g^{(j)}\}^{-e_j s}$$

if  $\operatorname{Re} s > 1$ . Here the sum is over a complete set of representatives for the equivalence relation on pairs  $g = (g_1, g_2)$  of elements of  $\mathfrak{a}$  given by  $(g_1, g_2) \sim (\varepsilon g_1, \varepsilon g_2)$

for  $\epsilon$  in  $U_K$ , the units of  $K$ . Tamagawa [11] and Ramanathan [6] both obtain the analytic continuation and functional equation of such functions by Hecke's method for the Dedekind zeta function. The Fourier expansion which we derive in [13] looks like the result quoted above in the case  $K = \mathbb{Q}$ , except that products of the special functions arise. Some trickery then yields the theorem stated in §1. For example, you must add up  $Z^a(P, s)$  over representatives  $a$  of ideal classes of  $K$  in order to get the Dedekind zeta function in the constant term of the Fourier expansion.

#### REFERENCES

1. A. Borel and G.D. Mostow, eds., Algebraic Groups and Discontinuous Subgroups, Proc. Symp. Pure Math., 9, A.M.S., Providence, R.I., 1966.
2. E. Grosswald, Relations Between the Values at Integral Arguments of Dirichlet Series that Satisfy Certain Functional Equations, Proc. Symp. Pure Math., 24, A.M.S., Providence, R.I., 1973.
3. T. Kubota, Elementary Theory of Eisenstein Series, Wiley, New York, 1973.
4. H. Maass, Lectures on Modular Functions of One Complex Variable, Tata Institute, Bombay, India, 1964.
5. J. Martinet, Artin L-Functions, Durham Symposium.
6. K.G. Ramanathan, Zeta Functions of Quadratic Forms, Acta Arithmetica, 7 (1961/62), 39-69.

7. K. Ribet, Deligne's Method for Proving Congruences Between L-Values, Durham Symposium.
8. C.L. Siegel, Lectures on Advanced Analytic Number Theory, Tata Institute, Bombay, India, 1957.
9. H.M. Stark, On the Problem of Unique Factorization in Complex Quadratic Fields, Proc. Symp. Pure Math., 12, A.M.S., Providence, R.I., 1969.
10. \_\_\_\_\_, Some Effective Cases of the Brauer-Siegel Theorem, Inventiones Math., 23 (1974), 135-152.
11. T. Tamagawa, On Some Extensions of Epstein's Z-series, Proc. Internatl. Symp. on Alg. No. Theory, Tokyo-Nikko (1955), 259-261.
12. A. Terras, Bessel Series Expansions of the Epstein Zeta Function and the Functional Equation, T.A.M.S., 183 (1973), 477-486.
13. \_\_\_\_\_, The Fourier Expansion of Epstein's Zeta Function over an Algebraic Number Field and its Consequences for Algebraic Number Theory, to appear in Acta Arithmetica, 1977.
14. H. Weyl, Selecta, Birkhauser Verlag, Basel and Stuttgart, 1960, pp. 521-553.
15. L.J. Mordell, On Hecke's Modular Functions, Zeta Functions, and Some other Analytic Functions in the Theory of Numbers, Proc. London Math. Society (2), 32 (1931), 501-556.
16. C.L. Siegel, Gesammelte Abhandlungen, I, Springer Verlag, New York, 1966, pp. 173-179 (Neuer Beweis die Funktionalgleichung der Dedekindschen Zetafunktion II, 1922).

Some Global Norm Density Results obtained from an  
Extended Čebotarěv Density Theorem

R. Odoni

Introduction

The intention here is to report on some recent work applying a modification of the well-known density theorem of Čebotarěv ([1], p.133) to various counting problems in algebraic number fields; in [2], I obtained an asymptotic expansion for the number of integers in a large interval which are  $K/\mathbb{Q}$  - norms of elements of  $K$  (an arbitrary algebraic number field), and, in [3] (resp. [4]), I obtained the corresponding expansion for  $K/\mathbb{Q}$  - norms of integers of  $K$  (respectively, integers in a fixed full module of  $K$ ). I propose to explain in outline how analogous results may be obtained for the following

Problem 1. Let  $(M_i)_{i \in I}$  be a finite collection of full modules, with  $M_i \subseteq \mathcal{O}_i$ , the ring of integers of some

algebraic number field  $K_i$ . Determine the number of rational integers in  $[1, x]$  which are in  $\bigcap_{i \in I} N_{K_i/\mathbb{Q}}[M_i]$ .

We remark that we may characterise  $\bigcap_{i \in I} N_{K_i/\mathbb{Q}}[M_i]$  as the set of rational integers simultaneously integrally represented by each of the Diophantine forms

$f_i(x_{i1}, \dots, x_{in_i})$ , on choosing  $\mathbb{Z}$ -bases  $\xi_{ij}$  for the  $M_i$ , and putting

$$f_i(x_{i1}, \dots, x_{in_i}) = N_{K_i/\mathbb{Q}} \left( \sum_j x_{ij} \xi_{ij} \right), \quad (1)$$

where  $n_i = [K_i:\mathbb{Q}]$ .

The solution is given by

Theorem 1. There exists a constant  $C = C((M_i))$  such that

$$\text{card } [1, x] \cap \bigcap_{i \in I} N_{K_i/\mathbb{Q}}[M_i] = Cx (\log x)^{E-1} + O(x(\log x)^{E-F-1}), \quad (2)$$

where  $F = F((M_i)) > 0$ , and  $E$  is the Dirichlet density of the set of rational primes which admit in each  $K_i$  at least one prime ideal factor of residual degree unity.

(It is easy, by considering the Galois hull over  $\mathbb{Q}$ , of the composite field  $\prod K_i$ , to see that  $E$  always exists and is

positive).

The constant implied by the  $O$ -symbol will generally depend on the choice of the  $M_i$ .

### §1. The reduction of Problem 1

We decompose the proof of Theorem 1 into several stages; the object is ultimately to imitate the famous proof of Landau [5] that

$$\sum_{\substack{1 \leq n \leq x \\ n=a^2+b^2}} 1 = c \cdot x / \sqrt{\log x} + O(x \cdot (\log x)^{-3/2}). \quad (3)$$

However, we shall have to work quite hard to reduce the problem to the right form.

The first snag is that, in general,  $\bigcap_{i \in I} N_{K_i/\mathbb{Q}}[M_i]$  has no particular multiplicative structure. This is not too disastrous; we can employ a trick (due in essence to H. Weber [6], and Fueter [7], in the case where the  $M_i$  are orders) which, roughly speaking, "approximates  $M_i$  by an ideal  $F_i \subseteq \mathcal{O}_i$ ". In fact, we define the conductor  $F_i$  of  $M_i$  to be the largest ideal of  $\mathcal{O}_i$  which is contained in  $M_i$ . An elementary piece of analysis (see [4]) now reduces the problem in Theorem 1 to that of solving

Problem 2. How many integers  $m$  are there in  $[1, x]$  which are simultaneously expressible as  $m = N_{K_i/\mathbb{Q}}(a_i)$ , where  $a_i \in \mathcal{O}_i$  is prime to  $F_i$  and is in one of a prescribed collection of congruence classes  $(\text{mod}^X F_i)$ ?

By introducing on the class of all subsets of the Cartesian product  $X_i \Gamma_i$  of the maximal ideal class groups  $(\text{mod}^X F_i)$  a semigroup structure  $\circ$ , whereby  $(X_i A_i) \circ (X_i B_i) = X_i A_i B_i$  with  $A_i B_i = \{a_i b_i; a_i \in A_i, b_i \in B_i\}$ , and by some unpleasant combinatorial arguments (cf. [3]), we can express the counting function in Problem 2 as a multiple contour integral involving a rational function in variables  $z_1, \dots, z_N$  (arising from a combinatorial generating function), and some Euler products  $\prod_{p \in P} (1 - z_j p^{-s})^{-1}$ ,  $(\text{Re } s > 1)$ , for various sets  $P$  of primes. The behaviour of these Euler products near  $s = 1$  is governed by the corresponding sums  $\sum_{p \in P} p^{-s}$ , and this is where the extended Čebotarěv theorem is wanted. Specifically, we need

Theorem 2. (Extended Čebotarěv theorem). Let  $(K_i)_{i \in I}$  be a finite collection of algebraic number fields, with  $F_i$  a conductor in  $K_i$ . Let  $P$  be the set of rational primes which



have, in each  $K_i$ , a specified number of prime ideal factors of specified residual degrees in specified classes  $(\text{mod}^x F_i)$ . Then  $P$  is either finite (possibly empty), or has positive rational Dirichlet density.

We shall prove this result in detail as it is of some independent interest. Let  $(H_i)_{i \in I}$  be the collection of class fields over the  $K_i$  corresponding to, say, the maximal ideal class groups  $(\text{mod}^x F_i)$ . Let  $H$  be their compositum  $\Pi H_i$ ;  $H$  may not be normal over  $\mathbb{Q}$ , so let  $\bar{H}$  be the Galois hull of  $H$  over  $\mathbb{Q}$ ; then  $H \supseteq K = \Pi K_i$ , so that  $\bar{H} \supseteq \bar{K}$ , the Galois hull of  $K$  over  $\mathbb{Q}$ . To prove our Čebotarěv theorem we consider two rational primes  $p \neq q$ , both unramified in  $\bar{H}$ , and assume that they determine the same Frobenius class in  $\text{Gal}(\bar{H}/\mathbb{Q})$ . It will then suffice to show that  $p$  and  $q$  decompose in the same way in each  $K_i$ , and that they have the same number of factors of given residual degree and class  $(\text{mod}^x F_i)$ .

Since  $p, q$  determine the same conjugacy class in  $\text{Gal}(\bar{H}/\mathbb{Q})$  we can label their respective divisors in  $\bar{H}$  as  $p_r, q_r$ , say, ensuring that the Frobenius symbols

$$\left[ \frac{\bar{H}/\mathbb{Q}}{p_r} \right] = \left[ \frac{\bar{H}/\mathbb{Q}}{q_r} \right], \quad \forall r. \quad (5)$$

Taking the natural projection of  $\text{Gal}(\bar{H}/Q)$  onto any of the  $\text{Gal}(\bar{K}_i/Q)$ , we deduce that

$$\left[ \frac{\bar{K}_i/Q}{p_r \cap \bar{K}_i} \right] = \left[ \frac{\bar{K}_i/Q}{q_r \cap \bar{K}_i} \right], \quad \forall r, i. \quad (6)$$

It follows that  $p$  and  $q$  decompose into the same number of factors of given residual degree in  $K_i$ , whatever our choice of  $i \in I$ . (see [1], p.123-126). We also have

$$\left[ \frac{\bar{H}/K_i}{p_r} \right] = \left[ \frac{\bar{H}/K_i}{q_r} \right], \quad \forall r, i, \quad (7)$$

since these Frobenius symbols both equal the smallest power of the symbol in (5) which lies in  $\text{Gal}(\bar{H}/K_i)$ . Now  $H_i/K_i$  is normal (indeed, abelian!) so, from (7), we can project down onto  $\text{Gal}(H_i/K_i)$ , obtaining

$$\left[ \frac{H_i/K_i}{p_r \cap H_i} \right] = \left[ \frac{H_i/K_i}{q_r \cap H_i} \right], \quad \forall r, i. \quad (8)$$

But the Frobenius symbols in (8) are actually the Artin symbols

$$\left( \frac{H_i/K_i}{p_r \cap K_i} \right) = \left( \frac{H_i/K_i}{q_r \cap K_i} \right), \quad \forall r, i. \quad (9)$$

Thus, by Artin's reciprocity theorem,  $p_r \cap K_i$  and  $q_r \cap K_i$  lie in the same class  $(\text{mod } {}^x F_i)$ , and we are done.

Of course, by relating the appropriate Artin L-functions to various abelian L-functions (using induced representations), we get a quantitative version of our theorem:

$$\sum_{p \in P} p^{-s} = d(P) \log \frac{1}{s-1} + f(s) \quad (10)$$

with  $f$  regular and explicitly boundable in some common zero-free region of the L-functions. We need this observation to solve Problem 2.

The resolution of Problem 2 is now in sight. The multiple contour integral mentioned above turns out to have a pole-factor which separates variable-by-variable, so we are spared the need to invoke the general form of Grothendieck's residue theorem; the remaining integral involves  $s$  (the variable in the Dirichlet series) breaks up as a sum of terms of the type

$$\int_{C-i\infty}^{C+i\infty} \frac{x^s}{s^2} (s-1)^{-\alpha} ds \quad (C > 1)$$

for various fractional exponents  $\alpha$ , and the final stages in solving Problem 2 are much the same as in [3].

## §2. An interesting special case and an unsolved problem

Suppose we are given various binary integral quadratic forms  $f_i$ , of discriminants  $D_i = d_i Q_i^2$ , where  $d_i$  is a field discriminant and we assume that the forms are neither zero-forms nor negative-definite. The procedure used in [4] (and in many works by earlier authors) shows that Theorem 1 can be applied to count the integers in  $[1, x]$  which are simultaneously integrally represented by all the  $f_i$ . In precise terms, if there exist integers  $m$  prime to all the  $2D_i$  for which the genus characters of  $m$  and the  $f_i$  all coincide, then there is a positive constant  $c$  (depending on the  $f_i$ ) such that

$$\text{card}[1, x] \cap \bigcap_i f_i[\mathbb{Z}^2] = cx(\log x)^{E-1} + O(x(\log x)^{E-F-1}) \quad (11)$$

(We remark that, in some circumstances, the constant  $C((M_i)_{i \in I})$  may be 0 in Theorem 1).

It is possible to obtain this result by another route, involving the extended Čebotarev result and some ingenious elementary ideas of P. Bernays (Göttingen Inaugural-dissertation, 1912). Indeed, this approach gives us the interesting extra result that "almost all" (in the sense of relative natural density) the integers prime to  $2\prod D_i$  which have the right genus characters for the  $f_i$  are represented

integrally by all the forms in the same genera as the  $f_i$ ,  
for all  $i \in I$ .

It would be of some interest to know for which fields  $K_i$  and which modules  $M_i$  we could expect a similar phenomenon to occur (with the appropriate definition of genus). This is clearly not an easy problem, even when only one field is involved. For instance, let us take an apparently simple case, where we have one field  $K$  and one module  $M = 0$ , the ring of integers of  $K$ . We consider the integers  $m \in [1, x]$  for which  $m = N\alpha$  for some ideal  $\alpha \subseteq 0$  in a specified narrow ideal class of  $K$ . Two ideals  $\alpha_1, \alpha_2$  with the same norm cannot be in completely arbitrary classes, since  $N\alpha_1\alpha_2^{-1} = 1$  and  $\alpha_1\alpha_2^{-1}$  therefore belongs to the subgroup  $H$  of classes which contain fractional ideals of norm unity, i.e.

$\alpha_1 H = \alpha_2 H$ . We might ask to compare  $S = \sum 1$ , taken over norms of ideals of class  $C$  (and with norm  $\leq x$ ), and the corresponding sum  $S^+$ , taken over the subset of these norms which arise from the full coset  $CH$  of classes. For which  $K$  are these asymptotically the same? To date, I cannot give a satisfactory answer to this question; the answer is however affirmative for the following special cases:

(1)  $K$  normal over  $\mathbb{Q}$ . (This explains the result for

integers simultaneously represented by quadratic forms, described above). The proof in this case seems to be due to the transitivity of the action of  $\text{Gal}(K/\mathbb{Q})$  on the prime ideals over a given rational prime.

(2)  $K$  any field with  $[K:\mathbb{Q}] = m$  and  $[\bar{K}:\mathbb{Q}] = mq$ , where  $q$  is a prime and  $q \nmid m$ . Thus, in particular,  $K$  any cubic field, and also any quartic field with  $\text{Gal}(\bar{K}/\mathbb{Q}) \cong A_4$ .

(I am indebted to T. Callaghan (Toronto) for remarks in the course of the conference which have enabled me to isolate this second category of fields).

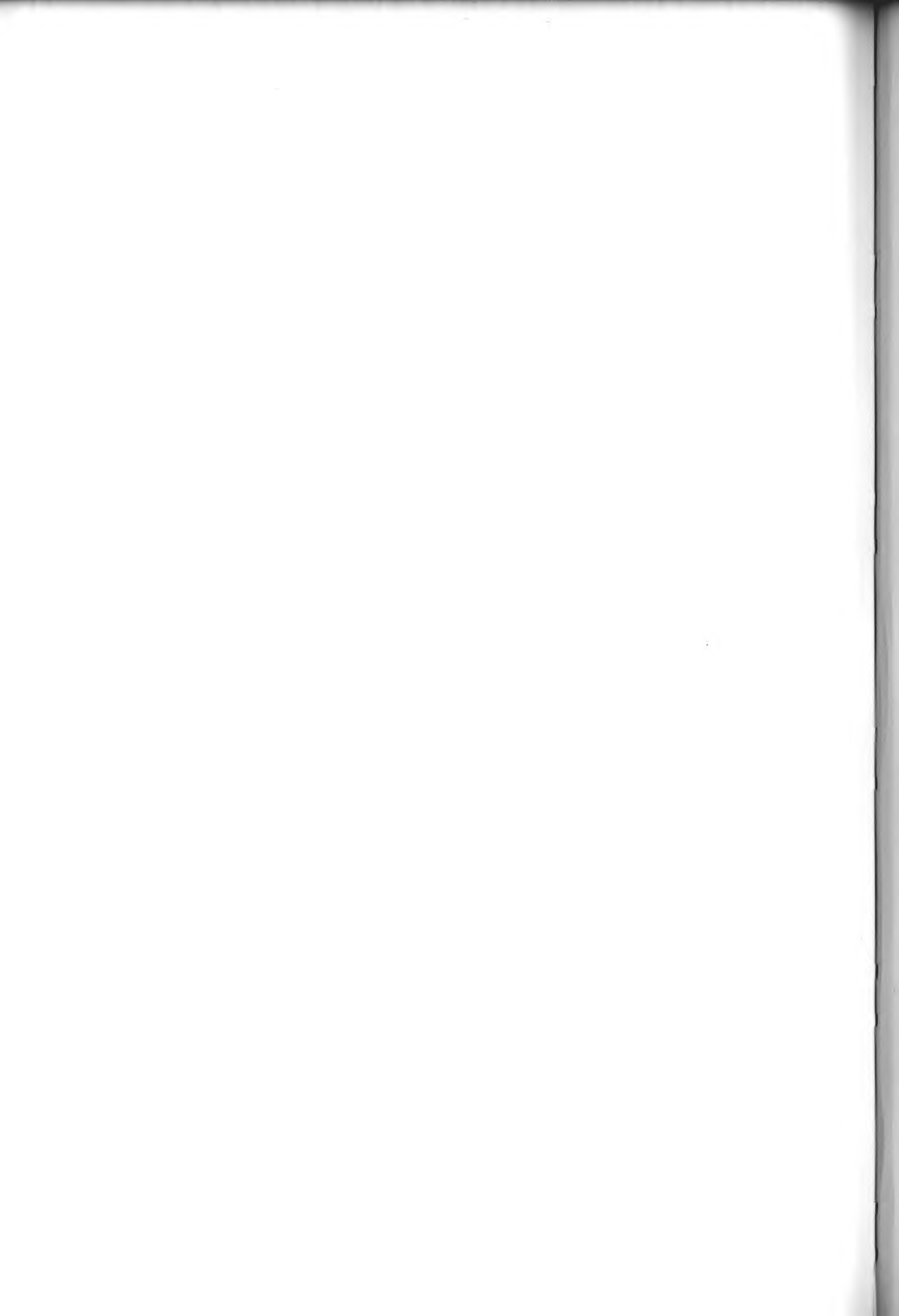
I would expect there to exist a quartic field giving a negative answer to the above question, but I have not found one.

#### REFERENCES

1. H. Hasse Bericht.....Theorie der Algebraischen Zahlkörper, Teil 2, (Physica Verlag, Würzburg, 1970).
2. R. Odoni "The Farey density of norm groups of global fields-I", Mathematika, 20 (1973), 155-169.
3. R. Odoni "On the norms of algebraic integers", Mathematika, 22 (1975), 71-80.
4. R. Odoni "On norms on integers in a full module.....", Mathematika, 22 (1975), 108-111.

5. E. Landau Handbuch der Primzahlverteilung (Teubner, Leipzig, 1909), Teil 2, 643-650.
6. H. Weber Lehrbuch der Algebra, (Braunschweig, 1908), vol.III.
7. R. Fueter "Die Klassenkorper der komplexe Multiplikation .....", Jahresbericht d. D.M.V. 20, (1911).





# A Survey of Class Groups of Integral Group Rings

Stephen V. Ullom<sup>\*</sup>

## Introduction

In this article we give a survey<sup>\*\*</sup> of the class group of locally free modules over integral group rings. Principally Jacobinski and Swan (see references) are responsible for the general outline. The recent developments deal with refinements and effective techniques of computation, which make the general theory more useful for applications. In topology C.T.C. Wall [W 1] defined an obstruction (in the projective class group of the fundamental group) to finding a finite complex in the homotopy type of a given space. Locally free modules are one of the

---

<sup>\*</sup> Work on this survey partially supported by an NSF grant.

<sup>\*\*</sup> The list of references contains all articles known to the author which deal specifically with class groups of integral group rings. Reiner's lectures [R 4] on this topic contain background material on orders also.

main objects of study in Galois module problems [F6] of algebraic number theory.

# §1. Definitions and formal properties of the locally free class group

Let  $G$  be a finite group and  $R$  the ring of all algebraic integers in a finite extension  $K$  of the rationals  $\mathbb{Q}$ . We consider modules over the group ring  $RG$  or more generally  $\Lambda$ -modules,  $\Lambda = R$ -order in a finite-dimensional semisimple  $K$ -algebra  $A$ . Let  $M$  be an  $R$ -lattice (finitely generated torsion free  $R$ -module) spanning a  $K$ -vector space  $V$ . The expression prime  $p$  of  $R$  shall mean either a maximal ideal  $p$  of  $R$  or an archimedean prime of  $K$ , and the subscript  $p$  denotes completion at  $p$ , e.g.  $M_p$ . We view  $M_p$   $V_p$  and set  $M_p = V_p$  for archimedean  $p$ . Let  $X^n$  be the sum of  $n$  copies of a module  $X$ .

(1.1) Definition Let  $M$  be an  $R$ -lattice and left  $\Lambda$ -module.  $M$  is locally free of rank  $n$  if  $M_p \cong \Lambda_p^n$  for each prime  $p$  of  $R$ . We then write  $\text{rk } M = n$ .

(1.2) Example Let  $N$  be a finite normal extension of  $K$ ,  $G = \text{Gal}(N/K)$ , and  $\Lambda = RG$ . A classical result of E. Noether asserts the ring of integers  $O_N$  of  $N$  is a locally free  $\Lambda$ -module if and only if  $N/K$  is tamely ramified.

Locally free implies projective. To see this recall  $M$  is  $\Lambda$ -projective if and only if  $\text{Ext}_{\Lambda}^1(M, L) = 0$  for all  $\Lambda$ -modules  $L$ , and the functor  $\text{Ext}$  commutes with localization in this setting ( $M$  assumed finitely generated hence finitely presented). Conversely, if  $\Lambda = RG$ , Swan [Sw 1] showed essentially that projective implies locally free.

(1.3) Definition  $K_0(\Lambda)$  = Grothendieck group of category of finitely generated locally free  $\Lambda$ -modules =  $F/F_0$ , where  $F$  = free abelian group on isomorphism classes  $\{M\}$  of locally free modules,  $F_0$  = subgroup generated by expressions  $\{M \oplus N\} - \{M\} - \{N\}$ .

Let  $(M)$  be the image of  $M$  in  $K_0(\Lambda)$ ;  $(M) = (N)$  if and only if  $M \oplus \Lambda^k \cong N \oplus \Lambda^k$  some  $k$ . Thus  $K_0(\Lambda)$  is the group of stable isomorphism classes of locally free  $\Lambda$ -modules.

(1.4) Definition The locally free class group

$\text{Cl } \Lambda = \ker(\text{rk} : K_0(\Lambda) \rightarrow \mathbb{Z})$ . Note any element of  $\text{Cl } \Lambda$  has the form  $(M) - (\Lambda^{\text{rk } M})$ .

A homomorphism  $\Lambda \rightarrow \Gamma$  of  $R$ -orders induces mapping

$\text{Cl } \Lambda \rightarrow \text{Cl } \Gamma$  by  $\Gamma \otimes_{\Lambda}$ . Two important examples follow.

1. If  $H$  is a subgroup of  $G$ , then  $\text{Cl } RH \rightarrow \text{Cl } RG$  by induction.

2. Let  $\Lambda' \supset \Lambda$  be a maximal  $R$ -order in  $A$ . Swan [Sw 4] proved  $\text{Cl } \Lambda \rightarrow \text{Cl } \Lambda'$  is onto. Denote by  $D(\Lambda)$  the kernel of this mapping. We shall see that  $D(\Lambda)$  is independent of the choice of maximal order and in fact has an invariant description.

Since  $\text{Cl } \Lambda' \cong$  product of (narrow) ideal class groups of the center of  $\Lambda'$  (see e.g. [Sw 3]), we may in one sense concentrate on  $D(\Lambda)$ . In applications, interesting invariants often lie in  $D(\Lambda)$ . For example, if  $N/Q$  is a normal tamely ramified extension with Galois group  $G$ , Fröhlich [F6] has proved Martinet's conjecture:

$$(O_N) - (ZG) \in D(ZG).$$

Also  $D(ZG)$  contains the subgroup  $T(ZG)$  described in §3.

Let  $R_K(G)$  be the character ring formed of K-characters of  $G$ .

(1.5) Theorem (i) A homomorphism of R-orders  $\Lambda \rightarrow \Gamma$  induces a map  $D(\Lambda) \rightarrow D(\Gamma)$ .

(ii) Let  $H$  be a subgroup of  $G$ , then the restriction map sends  $D(RG) \rightarrow D(RH)$ . Moreover,  $D(RG)$  is a Frobenius module for the Frobenius functor  $R_K(G)$  (see e.g. [Sw E, chap. 2] for terminology).

References Part (i) is due to Reiner [R 3] and part (ii) to Matchett [Mat]. Swan ([Sw 1], [Sw 4]) proved  $Cl(RG)$  is a Frobenius module over  $R_K(G)$ .

We now give Endo-Miyata's [EM 2] characterization of  $D(\Lambda)$ , which shows  $D(\Lambda)$  independent of maximal order and gives an alternative proof of (1.5).

(1.6) Theorem Let  $M$  be a locally free  $\Lambda$ -module of rank  $n$ . The element  $(M) - (\Lambda^n) \in Cl \Lambda$  belongs to  $D(\Lambda)$  if and only if there exists a finitely generated  $\Lambda$ -module  $X$  such that  $M \oplus X \cong \Lambda^n \oplus X$ . ( $X$  is not necessarily locally free.)

The proof depends on the lemma.

(1.7) Lemma Let  $M$  be a locally free  $\Lambda$ -module of rank  $n$ ,  $\Lambda' \supset \Lambda$  a maximal  $R$ -order, then

$$M \oplus \Lambda'^n \cong [\Lambda' \otimes_{\Lambda} M] \oplus \Lambda^n \quad \text{as } \Lambda\text{-modules.}$$

Proof Let  $S =$  (finite) set of prime ideals  $p$  of  $R$  such that  $\Lambda_p \neq \Lambda'_p$ . By Roiter's lemma ([Sw E, (3.1)] or [R 2, (27.1)]) there exists an exact sequence of  $\Lambda$ -modules

$$0 \rightarrow M \rightarrow \Lambda^n \rightarrow T \rightarrow 0$$

with  $T_p = 0$  for  $p \in S$ . Note that  $\Lambda' \otimes_{\Lambda} T \cong T$ , so the sequence below is exact

$$0 \rightarrow \Lambda' \otimes_{\Lambda} M \rightarrow \Lambda'^n \rightarrow T \rightarrow 0 \quad .$$

Again by Roiter [Sw E, Lemma 6.9]

$$M \oplus \Lambda'^n \cong [\Lambda' \otimes_{\Lambda} M] \oplus \Lambda^n \quad . \quad \text{Q.E.D.}$$



Returning to the proof of (1.6), we see that if  $(M) - (\Lambda^n) \in D(\Lambda)$ , then  $\Lambda'^k \oplus [\Lambda' \otimes_{\Lambda} M] \cong \Lambda'^{n+k}$  for some  $k$ , so from the lemma

$$M \oplus \Lambda'^{n+k} \cong \Lambda^n \oplus \Lambda'^{n+k}.$$

We have proved one direction of the theorem with  $X = \Lambda'^{n+k}$ . The other direction is almost obvious.

Remarks Continuing with the philosophy that one should look at subgroups and quotient groups of  $Cl(RG)$ , Fröhlich ([F 5], [F 6]) has defined certain quotients of  $D(ZG)$  called the E-groups, which are useful in the normal integral basis problem. Also Endo-Miyata [EM 1,2,3] have considered other subgroups of  $D(ZG)$  which are Frobenius modules.

## §2. Methods of computation

To begin with  $Cl \Lambda$  is a finite abelian group. Indeed Swan has proved [Sw 1] that if  $M$  is a locally free  $\Lambda$ -module, then  $M \cong (\text{free } \Lambda\text{-module}) \oplus (\text{locally free left ideal of } \Lambda)$ . It follows every element of  $Cl \Lambda$  can be written in the form  $(M) - (\Lambda)$  for some locally free left ideal  $M$  of  $\Lambda$ . Hence by

the Jordan-Zassenhaus theorem [CR §79] Cl  $\Lambda$  is finite.

Next we describe the class group explicitly as a quotient of an idele group. (Compare Jacobinski's original classification ([J 1], [J 2]) of lattices in a given genus.) For a ring  $S$ ,  $u(S)$  denotes the group of invertible elements of  $S$ . Define the ideles  $J(A) \subset \prod u(A_p)$ , product over all primes  $p$  of  $R$ , by

$$J(A) = \{(\alpha_p) \in \prod u(A_p) : \alpha_p \in u(\Lambda_p) \text{ for all but finitely many } p\}.$$

Let  $U(\Lambda) = \prod u(\Lambda_p)$ . The idele group  $J(A)$  is topologized so that  $U(\Lambda)$  is an open subgroup with its subgroup topology the same as the product topology. Let  $J(A)'$  be the closure of the commutator subgroup of  $J(A)$  and embed  $A$  diagonally in  $J(A)$

For  $\alpha = (\alpha_p) \in J(A)$  define

$$\Lambda\alpha = \bigcap_p (\Lambda_p \alpha_p \cap A);$$

$\Lambda\alpha$  is a locally free  $\Lambda$ -module in  $A$ . Conversely, let  $M$  be a locally free rank 1  $\Lambda$ -module in  $A$  with  $M_p = \Lambda_p \alpha_p$ ,  $\alpha_p \in u(A_p)$ . Set  $\alpha = (\alpha_p)$ . Then  $\alpha \in J(A)$  and  $M = \Lambda\alpha$ .

(2.1) Proposition There is a 1-1 correspondence between isomorphism classes of locally free rank 1 left  $\Lambda$ -modules in  $A$  and double cosets  $U(\Lambda) \backslash J(A) / u(A)$  given by

$$\{\Lambda\alpha\} \leftrightarrow U(\Lambda)\alpha u(A), \quad \alpha \in J(A).$$

(2.2) Theorem (Fröhlich [F 4]). The mapping  $(\Lambda\alpha) - (\Lambda) \rightarrow \alpha \bmod J(A)' U(\Lambda) u(A)$  defines an isomorphism

$$(2.3) \quad Cl \Lambda \rightarrow J(A) / J(A)' U(\Lambda) u(A),$$

which is natural in homomorphisms of R-orders.

Fröhlich's approach gives an explicit condition which is both necessary and sufficient for an order to have the cancellation property for locally free modules. In particular,  $\Lambda$  has the cancellation property provided none of the simple components of  $A$  is a totally definite quaternion algebra (i.e.  $A$  satisfies the "Eichler condition"). The main technical point of the proof is that if  $B$  is a simple  $\mathbb{Q}$ -algebra,  $B$  not a totally definite quaternion algebra, then  $J(B)'$  has strong approximation.

Often one applies the reduced norm to the right hand side of (2.3). Further notation is needed. Let

$$A = \sum A_i, \quad A_i \text{ simple } K\text{-algebra with center } L_i$$

$$L = \sum L_i = \text{center of } A$$

$$O = \sum O_{L_i}, \quad O_{L_i} = \text{ring of integers of } L_i.$$

The reduced norm  $n_i$  maps  $A_i \rightarrow L_i$  and we also have reduced norms  $n : A \rightarrow L$  and  $n : J(A) \rightarrow J(L)$  defined componentwise and locally (resp.). Let  $\mathbb{H}$  be the skewfield of real quaternions and set

$$J(L_i)_+ = \{(\beta_P) \in J(L_i) : \beta_P > 0 \text{ if } P \text{ is a real archimedean}$$

prime of  $L_i$  such that  $A_{i,P}$  is a matrix ring over  $\mathbb{H}$  }.

Let  $J(L)_+ = \sum J(L_i)_+$  and for any subset  $S \subset J(L)$  define  $S_+ = S \cap J(L)_+$ . Using results on the image of reduced norm (locally and globally) and  $\ker(n : J(A) \rightarrow J(L)) = J(A)'$  Fröhlich [F 4] proves the following.

(2.4) Theorem      The reduced norm gives an isomorphism

$$J(A)/J(A)' \cap U(\Lambda) \cap u(A) \cong J(L)_+ / n(U(\Lambda)) \cap u(L)_+$$

$$\cong J(L)/n(U(\Lambda)) \cap u(L).$$

Further  $n(U(\Lambda))$  is an open subgroup of  $J(L)$ .

(2.5) Corollary  $D(\Lambda) \cong U(0)_+ \cap u(L)/n(U(\Lambda)) \cap u(L)$ , (since  $n(U(\text{maximal order})) = U(0)_+$ ).

C.T.C. Wall and S. Wilson have given similar idele descriptions of  $Cl \Lambda$  (actually for more general rings) by techniques of algebraic K-theory. We indicate briefly one of the ideas Wall uses in the course of his classification of Hermitian forms over adèle rings and global rings. Let  $\hat{Z}$  = profinite completion of  $Z$ ,

$$\hat{Q} = Q \otimes_Z \hat{Z}, \quad \hat{\Lambda} = \Lambda \otimes_Z \hat{Z}, \quad \hat{A} = \Lambda \otimes_Z \hat{Q}.$$

From the Mayer-Vietoris sequence of the fiber product

$$\begin{array}{ccc} \Lambda & \longrightarrow & A \\ \downarrow & & \downarrow \\ \hat{\Lambda} & \longrightarrow & \hat{A} \end{array}$$

Wall ([W 2, Cor. 2.2], [W 3, Cor. 3.2]) proves (2.6) below. Wilson ([Wi 3], [R 4]) has proved (2.6) independently by the localization sequence of algebraic K-theory.

(2.6) Theorem The class group  $Cl \Lambda \stackrel{\sim}{=} X/Y$ , where  $X =$  restricted direct product of the groups  $K_1(A_p)$  with respect to the subgroups

$$\text{im } K_1(\Lambda_p) = \text{image } (K_1(\Lambda_p) \rightarrow K_1(A_p)) \quad .$$

And  $Y = \text{im } K_1(A) \cdot \text{im } \prod K_1(\Lambda_p)$ . Here  $p$  ranges over all finite rational primes.

An adaptation of Milnor's [M] Mayer-Vietoris sequence to orders is a useful technique for computing class groups of specific orders. Given  $R$ -orders  $\Lambda, \Lambda_1, \Lambda_2$  in semisimple  $K$ -algebras and a finite (as a set)  $R$ -algebra  $\bar{\Lambda}$ . Assume  $\Lambda$  is the fiber product

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda_1 \\ \downarrow & & \downarrow \phi_1 \\ & \phi_2 & \\ \Lambda_2 & \longrightarrow & \bar{\Lambda} \end{array} ,$$

i.e.  $\Lambda$  is identified with the subring

$$\{(\lambda_1, \lambda_2) \in \Lambda_1 \oplus \Lambda_2 : \phi_1 \lambda_1 = \phi_2 \lambda_2\}.$$

Let  $u^*(\Lambda_i) = \text{im}(u(\Lambda_i) \rightarrow u(\bar{\Lambda}))$ ,  $i = 1, 2$ .

(2.7) Theorem [RU 2, F 4]. Assume  $\phi_1$  or  $\phi_2$  is surjective.

(i) If  $A$  satisfies the Eichler condition, the following sequences are exact

$$1 \rightarrow u^*(\Lambda_1) \rightarrow u^*(\Lambda_2) \rightarrow u(\bar{\Lambda}) \rightarrow \text{Cl } \Lambda \rightarrow \text{Cl}(\Lambda_1) \oplus \text{Cl}(\Lambda_2) \rightarrow 1$$

$$1 \rightarrow u^*(\Lambda_1) \rightarrow u^*(\Lambda_2) \rightarrow u(\bar{\Lambda}) \rightarrow D(\Lambda) \rightarrow D(\Lambda_1) \oplus D(\Lambda_2) \rightarrow 1.$$

(ii) Whether or not  $A$  satisfies the Eichler condition, the above two sequences are exact with  $u(\bar{\Lambda})$  replaced by  $\text{GL}_2(\bar{\Lambda})$  and  $u^*(\Lambda_i)$  replaced by  $\text{im}(\text{GL}_2(\Lambda_i) \rightarrow \text{GL}_2(\bar{\Lambda}))$ ,  $i = 1, 2$ .

The idea behind the proof of (ii) is that  $M_2(A)$ , the ring of 2 by 2 matrices over  $A$ , obviously satisfies the Eichler condition. Also  $\text{Cl}(\Lambda) \cong \text{Cl}(M_2(\Lambda))$ ,  $D(\Lambda) \cong D(M_2(\Lambda))$ .



### §3. Numerical results

In §3, §4 we specialize to  $\Lambda = \mathbb{Z}G$ . Let  $C_m$  be the cyclic group of order  $m$  and  $|S|$  the cardinality of a set  $S$ .

(3.1) Theorem Suppose  $G$  is a  $p$ -group.

(i)  $([F\ 1], [RU\ 1])$ .  $D(\mathbb{Z}G)$  is a  $p$ -group.

(ii)  $[U\ 2]$ . The exponent of  $D(\mathbb{Z}G)$  divides  $|G|/p$  if  $p \neq 2$ , divides  $|G|/4$  if  $p = 2$ .

(3.2) Theorem As  $G$  ranges over a sequence of abelian groups such that  $|G| \rightarrow \infty$  ( $|G|$  not prime), then  $|D(\mathbb{Z}G)| \rightarrow \infty$ .

References Frohlich  $[F\ 2]$  determines the exact order of  $D(\mathbb{Z}G)^-$  (defined in §4) for an arbitrary abelian  $p$ -group  $G$ ,  $p \neq 2$ . On the other hand article  $[RU\ 2]$  gives lower bounds of  $|D(\mathbb{Z}G)^-|$  for any abelian group.

For an odd prime  $\ell$  define the metacyclic group  $\Omega = \Omega(\ell^r, q)$ ,  $r \geq 1$  and  $q$  any divisor of  $\ell - 1$ , by the extension

$$1 \rightarrow C_{\ell^r} \rightarrow \Omega \rightarrow C_q \rightarrow 1$$

where  $C_q$  acts faithfully on  $C_{\ell^r}$ .

(3.3) Theorem [GRU]. Suppose  $\Omega$  as above has order  $\ell q$ . Then  $D(Z\Omega) = D(ZC_q) \oplus C_{q'}$ ,  $q' = q/(q, 2)$ .

Work of Keating [K 2] with further contributions by Cassou-Noguès [CN 2] and independently Matchett [Mat] yield the following.

(3.4) Theorem Suppose  $\Omega$  as above has order  $\ell^r q$ . There is a split exact sequence

$$1 \rightarrow D_0(Z\Omega) \rightarrow D(Z\Omega) \rightarrow D(ZC_q) \rightarrow 1.$$

Further  $D_0(Z\Omega) \cong C_{q'}^{(r)} \oplus Y$ , where  $Y$  is an  $\ell$ -group and  $Y = 1$  if  $\ell$  is a regular\* prime.

The article by Cassou-Noguès [CN 2] has results on more general metacyclic groups.

---

\* A prime  $\ell$  is said to be regular if  $\ell$  does not divide the class number of the field  $Q(\sqrt[\ell]{1})$ .

Define the Artin exponent  $A(G)$  to be the characteristic of the quotient of the character ring  $R_Q(G)$  by the ideal generated by generalized characters coming by induction from cyclic subgroups of  $G$ . Lam's work [La] provides an effective method of computing  $A(G)$ . It is known that  $A(G)$  divides  $|G|$  and  $A(G) = 1$  if and only if  $G$  is cyclic. Except for the three exceptional families of 2-groups described below, one has  $A(G) = |G|/p$ , when  $G$  is a noncyclic  $p$ -group,  $p$  any prime [La]. These families are

$$(3.5) \quad \left\{ \begin{array}{l} \text{dihedral } \Delta_{2^{n+2}} = \langle \sigma, \tau : \sigma^{2^{n+1}} = \tau^2 = 1, \\ \qquad \qquad \qquad \tau^{-1} \sigma \tau = \sigma^{-1} \rangle, \quad n \geq 0 \\ \\ \text{quaternion } H_{2^{n+2}} = \langle \sigma, \tau : \sigma^{2^n} = \tau^2, \quad \tau^4 = 1, \\ \qquad \qquad \qquad \tau^{-1} \sigma \tau = \sigma^{-1} \rangle, \quad n \geq 1 \\ \\ \text{semidihedral } SD_{2^{n+2}} = \langle \sigma, \tau : \sigma^{2^{n+1}} = \tau^2 = 1, \\ \qquad \qquad \qquad \tau^{-1} \sigma \tau = \sigma^{-1+2^n} \rangle, \quad n \geq 2. \end{array} \right.$$

We have  $A(\Delta) = A(H) = 2$ ,  $A(SD) = 4$ .

(3.6) Theorem (i) [FKW]. We have  $D(Z\Delta) = 1$ ,  $|D(ZH)| = 2$ .

(ii) [E]. The semidihedral group  $SD \supset H_8$  and  $|D(ZSD)| = 2$ .

Let  $G$  be any of the three groups of (3.5). The proof of (3.6) begins with an application of the Mayer-Vietoris sequence of (2.7) to the fiber product

$$\begin{array}{ccc} ZG & \longrightarrow & ZG/(\sigma^{2^n} - 1) \stackrel{\sim}{=} Z\Delta_{2^{n+1}} \\ \downarrow & & \downarrow \\ ZG/(\sigma^{2^n} + 1) & \rightarrow & ZG/(2, \sigma^{2^n} - 1) \stackrel{\sim}{=} \mathbb{F}_2 \Delta_{2^{n+1}}. \end{array}$$

Remarks Martinet [Mar] proved there are exactly two non-isomorphic locally free rank 1  $ZH_8$ -modules. Wall [W 4], as an illustrative example, calculates the class group of the elementary abelian 2-group and the nonabelian groups of order 8.

Let  $H_{4p^r} = \langle \sigma, \tau : \sigma^{p^r} = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$  be the quaternion group of order  $4p^r$ ,  $p$  odd prime.

(3.7) Theorem ([F 3], [Wi 3]). The 2-component of  $D(ZH_{4p^r})$  is an elementary abelian group of order  $2^r$ .

We conclude this section with a description of the subgroup  $T(ZG)$  of  $D(ZG)$  introduced by Swan [Sw 2]. Its elements are used in the classification of fixed point free actions of groups on spheres (e.g. [LT], [TW]). Let  $n = |G|$ ,  $\Sigma_G = \Sigma = \text{sum of elements of } G$ ,  $\Sigma \in ZG$ . Form the fiber product

$$\begin{array}{ccc} ZG & \longrightarrow & ZG/(\Sigma) \\ \downarrow & & \downarrow \\ Z & \longrightarrow & Z/nZ \end{array} .$$

Then the sequence

$$u(Z/uZ) \xrightarrow{\partial} D(ZG) \rightarrow D(ZG/(\Sigma)) \rightarrow 1$$

is exact and  $\partial(r \bmod nZ) = ([r, \Sigma]) - (ZG)$ , integer  $r$  prime to  $n$ . Here  $[r, \Sigma] = \text{the locally free ideal } rZG + \Sigma \cdot ZG$ . Define  $T(ZG) = \text{im } \partial$ . Then  $T(ZG) \subset D(ZG)$ ; in fact

$$[r, \Sigma] \oplus Z \stackrel{\sim}{=} ZG \oplus Z \quad (\text{see [Sw 2]}) ,$$

so  $X = Z$  with trivial  $G$ -action in the notation of (1.6).

We state several results of Ullom [U 3]. The exponent

of  $T(ZG)$  divides  $A(G)$  and it is likely that the exact exponent of  $T(ZG)$  is either  $A(G)$  or  $A(G)/2$ .

1. Quotient. If  $G$  maps onto  $\bar{G}$ , then  $T(ZG)$  maps onto  $T(Z\bar{G})$ .

2. Restriction. Let  $H$  be a subgroup of  $G$ . The restriction map of class groups maps  $T(ZG)$  onto  $T(ZH)$  by

$$([r, \Sigma_G]) - (ZG) \rightarrow ([r, \Sigma_H]) - (ZH).$$

For the groups  $G$  of (3.3) (with  $q$  prime) and (3.5),

$T(ZG) = D(ZG)$ . There are general lower bounds for  $T(ZG)$  in terms of  $A(G)$ .

(3.8) Theorem [U 3]. An odd prime  $p$  divides  $|T(ZG)|$  if and only if  $p$  divides  $A(G)$ . If 4 divides  $A(G)$ , then  $|T(ZG)|$  is even, except possibly when a 2-Sylow subgroup of  $G$  is dihedral.

(3.9) Proposition (i) Let  $G = S_n$  or  $A_n$  (symmetric or alternating group on  $n$  letters). An odd prime  $p$  divides  $|T(ZG)|$  if and only if  $p \leq n/2$ .

(ii) An odd prime  $p$  divides  $|Cl(ZS_n)|$  if and only if

$p \leq n/2$ .  $|Cl(ZS_n)|$  is even if and only if  $n \geq 5$ .

References For the symmetric and alternating group see [EM 3], [R 3], [RU 4], and [U 3].

#### §4. Cyclic p-groups

Probably the deepest results on class groups deal with cyclic p-groups. Of course one purpose of the induction theorems is to reduce to this basic case. Both Kervaire-Murthy [KM] and Galovich [G] apply the theory of cyclotomic fields to class group problems. The former make systematic use of Iwasawa's theory in contrast to the latter's direct approach with cyclotomic units (mostly for p a regular prime). However, Galovich has pointed out that the proof of his claimed direct sum decomposition of  $D(ZG)$  is in error.

Let  $F_n = \mathbb{Q}(\omega_n)$ ,  $\omega_n$  = primitive  $p^{n+1}$ -st root of 1, and  $R_n = \mathbb{Z}[\omega_n]$ . Note that the class group of the maximal order of  $\mathbb{Q}C_{p^{n+1}}$  ( $C_m$  cyclic of order m) is isomorphic to the product  $\prod_{i=0}^n Cl(R_i)$  of ideal class groups. The fiber

product



$$(4.1) \quad \begin{array}{ccc} \mathbb{Z}C_{p^{n+1}} & \longrightarrow & \mathbb{Z}C_{p^n} \\ \downarrow & & \downarrow \\ R_n & \longrightarrow & \mathbb{F}_p^C C_{p^n} \end{array}$$

yields the exact Mayer-Vietoris sequence

$$(4.2) \quad u(\mathbb{Z}C_{p^n}) \times u(R_n) \xrightarrow{j_n} u(\mathbb{F}_p^C C_{p^n}) \rightarrow D(\mathbb{Z}C_{p^{n+1}}) \rightarrow D(\mathbb{Z}C_{p^n}) \rightarrow 1.$$

Define the standard involution  $c$  on  $\mathbb{Z}C$ ,  $C$  generated by  $\sigma$ , to be  $c(\sum a_i \sigma^i) = \sum a_i \sigma^{-i}$ ,  $a_i \in \mathbb{Z}$ . Let  $Y$  be any  $\langle c \rangle$ -module written multiplicatively and define

$$Y^+ = \{y \in Y : y^c = y\}, \quad Y^- = \{y \in Y : y^c = y^{-1}\}.$$

Since  $c$  acts on the fiber product (4.1), it follows easily that (4.2) is an exact sequence of  $\langle c \rangle$ -modules. From now on assume  $p$  odd, so  $D(\mathbb{Z}C) = D(\mathbb{Z}C)^+ \oplus D(\mathbb{Z}C)^-$ . (With more work [KM] handle the case  $p = 2$ .) Let  $V_n = \text{cokernel of } j_n$ .  $V_n$  is a  $p$ -group because the unit  $(1 - \omega_n^r)/(1 - \omega_n) \equiv r \pmod{(1 - \omega_n)R_n}$ ,  $(r, p) = 1$ . Two results on units are fundamental.

$$(4.3) \quad \underline{\text{Lemma}} \quad (i) \quad u(R_n) = \langle \omega_n \rangle u^+(R_n).$$

$$(ii) \quad u(ZC_{p^n}) = C_{p^n} \cdot u^+(ZC_{p^n}).$$

Part (i) is due to Kummer [KM]; for (ii) see [CR] and [KM]. On the other hand  $u^-(\mathbb{F}_p C_{p^n})$  is roughly one half of  $u(\mathbb{F}_p C_{p^n})$ . It follows that  $V_n^-$  is large. The structure of  $V_n^-$  as an abelian group is determined in [KM]. An important upper bound for  $V_n^+$  follows.

(4.4) Theorem [KM]. Assume that  $p$  is an odd prime such that  $(p, h_0^+) = 1$ , where  $h_0^+ =$  class number of the maximal real subfield of  $F_0$ . Let  $Cl(R_{n-1})_p^-$  be the subgroup of skew-symmetric elements of the  $p$ -primary subgroup of  $Cl(R_{n-1})$ . There is a canonical injection

$$\text{character group of } V_n^+ \rightarrow Cl(R_{n-1})_p^-.$$

Corollary If  $p$  is regular, then  $V_n^+ = 1$  and  $D(ZC_{p^{n+1}})^+ = 1$  for all  $n \geq 0$ .

Conjecture [KM]. Assume  $(p, h_0^+) = 1$ . Let  $\delta_p$  be the number

of Bernoulli numbers  $B_2, B_4, \dots, B_{p-3}$  with numerators divisible by  $p$ . Then

$$V_n^+ \cong \delta_p \text{ copies of } C_{p^n}.$$

For  $n = 1$  the conjecture has been proved by Galovich [G] and Kervaire-Murthy [KM].

In [U 4] Ullom investigates the  $\Delta$ -decomposition of the  $p$ -primary subgroup of  $Cl(ZG)$  and  $D(ZG)$ ,  $G$  a cyclic  $p$ -group. The "odd" eigenspaces under this decomposition contain as subgroups the corresponding eigenspaces of certain ray class groups of cyclotomic fields. Then one can apply results of Iwasawa [I] to show, for example, that  $D(ZC_{p^{n+1}})$  is not a direct summand of  $Cl(ZC_{p^{n+1}})$  if  $p$  is an irregular prime with  $(p, h_0^+) = 1$ ,  $n \geq 1$ .

#### REFERENCES

- CN 1 P. Cassou-Noguès, Classes d'ideaux de l'algebre d'un groupe abelien, C.R. Acad. Sci. Paris, 276 (1973), 973-975.
- CN 2 \_\_\_\_\_, Groupe des classes l'algebre d'un groupe metacyclique, (to appear).
- CR C.W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras, Pure and Appl. Math., vol. XI, Interscience,

New York, 1962, 2nd ed., 1966.

- E S. Endo, letter dated August 25, 1975.
- EM 1 S. Endo, T. Miyata, Quasi-permutation modules over finite groups I, J. Math. Soc. Japan, 25 (1973), 397-421.
- EM 2 \_\_\_\_\_, Quasi-permutation modules over finite groups II, J. Math. Soc. Japan, 26 (1974), 698-713.
- EM 3 \_\_\_\_\_, On the projective class group of finite groups (to appear).
- F 1 A. Fröhlich, On the classgroup of integral group rings of finite abelian groups I, Mathematika, 16 (1969), 143-152.
- F 2 \_\_\_\_\_, On the classgroup of integral group rings of finite abelian groups II, Mathematika, 19 (1972), 51-56.
- F 3 \_\_\_\_\_, Module invariants and root numbers of quaternion fields of order  $4\ell^r$ , Proc. Camb. Phil. Soc., 76 (1974), 393-399.
- F 4 \_\_\_\_\_, Locally free modules over arithmetic orders, J. für Math., 274/275 (1975), 112-124.
- F 5 \_\_\_\_\_, Arithmetic and Galois module structure for tame extensions, (to appear).
- F 6 \_\_\_\_\_, Galois module structure, Durham Symposium.
- FKW A. Fröhlich, M.E. Keating, S.M.J. Wilson, The class group of quaternion and dihedral 2-groups, Mathematika, 21 (1974), 64-71.
- G S. Galovich, The class group of a cyclic p-group, J. of Algebra, 30 (1974), 368-387.

- GRU S. Galovich, I. Reiner, S. Ullom, Class groups for integral representations of metacyclic groups, *Mathematika*, 19 (1972), 105-111.
- I K. Iwasawa, On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan*, 16 (1964), 42-82.
- J 1 H. Jacobinski, Über die Geschlechter von Gittern über Ordnungen, *J. für Math.*, 230 (1968), 29-39.
- J 2 \_\_\_\_\_, Genera and decompositions of lattices over orders, *Acta Math.*, 121 (1968), 1-29.
- K 1 M.E. Keating, On the K-theory of the quaternion group, *Mathematika*, 20 (1973), 59-62.
- K 2 \_\_\_\_\_, Class groups of metacyclic groups of order  $p^r q$ ,  $p$  a regular prime, *Mathematika*, 21 (1974), 90-95.
- KM M.A. Kervaire, M.P. Murthy, On the projective class group of cyclic groups of prime power order (to appear).
- La T. Y. Lam, Artin exponent of finite groups, *J. of Algebra*, 9 (1968), 94-119.
- Le M. P. Lee, Integral representations of dihedral groups of order  $2p$ , *Trans. Amer. Math. Soc.*, 110 (1964), 213-231.
- LT R. Lee, C. Thomas, Free finite group actions on  $S^3$ , *Bull. Amer. Math. Soc.*, 79 (1973), 211-215.
- Mar J. Martinet, Modules sur l'algèbre du groupe quaternion, *Ann. Sci. Ecole Norm. Sup.*, 4 (1971), 399-408.
- Mat A. Matchett, Bimodule-induced morphisms of class groups, *J. of Algebra* (to appear).

- M J. Milnor, Introduction to algebraic K-theory, Ann. of Math. Studies No. 72, Princeton Univ. Press, 1971.
- P L. C. Pu, Integral representations of non-abelian groups of order  $pq$ , Michigan Math. J., 12 (1965), 231-246.
- R 1 I. Reiner, A survey of integral representation theory, Bull. Amer. Math. Soc., 76 (1970), 159-227.
- R 2 \_\_\_\_\_, Maximal orders, Academic Press. London, 1975.
- R 3 \_\_\_\_\_, Projective class groups of symmetric and alternating groups, Linear and Multilinear Algebra, 3 (1975), 147-153.
- R 4 \_\_\_\_\_, Class groups and Picard groups of integral group rings and orders, Regional Conf. Math., Carleton College, August 1975 (to appear).
- RU 1 I. Reiner, S. Ullom, Class groups of integral group rings, Trans. Amer. Math. Soc., 179 (1972), 1-30.
- RU 2 \_\_\_\_\_, A Mayer-Vietoris sequence for class groups, J. of Algebra, 31 (1974), 305-342.
- RU 3 \_\_\_\_\_, Class groups of orders and a Mayer-Vietoris sequence, Springer Lecture Notes 353 (1973), 139-151.
- RU 4 \_\_\_\_\_, Remarks on class groups of integral group rings, Symp. Math. Ist. Nazionale Alta Mat. (Rome), 13 (1974), 501-516.
- Ri D.S. Rim, Modules over finite groups, Ann. of Math., 69 (1959), 700-712.

- Ro M. Rosen, Representations of twisted group rings,  
Ph. D. thesis, Princeton Univ., 1963.
- Sw 1 R.G. Swan, Induced representations of projective  
modules, Ann. of Math., 71 (1960), 552-578.
- Sw 2 ———, Periodic resolutions for finite groups,  
Ann. of Math., 72 (1960), 267-291.
- Sw 3 ———, Projective modules over group rings and  
maximal orders, Ann. of Math., 76 (1962),  
55-61.
- Sw 4 ———, The Grothendieck ring of a finite  
group, Topology, 2 (1963), 85-110.
- Sw 5 ———, Algebraic K-theory, Springer Lecture  
Notes 76, Berlin, 1968.
- SwE R.G. Swan, E.G. Evans, K-theory of finite groups  
and orders, Springer Lecture Notes 149,  
Berlin, 1970.
- TW C.B. Thomas, C.T.C. Wall, The topological  
spherical space form problem I, Compositio  
Math. 23 (1971), 101-114.
- U 1 S. Ullom, A note on the class group of integral  
group rings of some cyclic groups,  
Mathematika, 17 (1970), 79-81.
- U 2 ———, The exponent of class groups, J. of  
Algebra, 29 (1974), 124-132.
- U 3 ———, Nontrivial lower bounds for class groups  
of integral group rings, Illinois J. Math.,  
20 (1976), 361-371.
- U 4 ———, The  $\Delta$ -decomposition of the class group  
of cyclic  $p$ -groups (to appear).
- W 1 C.T.C. Wall, Finiteness conditions for CW-complexes,  
Ann. of Math., 81 (1965), 56-69.



- W 2 C.T.C. Wall, On the classification of Hermitian forms IV. Adele rings. *Inventiones math.*, 23 (1974), 241-260.
- W 3 ———, On the classification of Hermitian forms V. Global rings. *Inventiones math.*, 23 (1974), 261-288.
- W 4 ———, Norms of units in group rings, *Proc. London Math. Soc.*, (3) 29 (1974), 593-632.
- Wi 1 S.M.J. Wilson, K-theory for twisted group rings, *Proc. London Math. Soc.* (3), 29 (1974), 257-271.
- Wi 2 ———, Twisted group rings and ramification, *Proc. London Math. Soc.* (3), 31 (1975), 311-330.
- Wi 3 ———, Reduced norms in the K-theory of orders, *J. of Algebra* (to appear).

# H<sub>8</sub>

J. Martinet

Theorem 5.1. of [M1] shows that quaternion extensions play a crucial role in the study of conductors and root numbers of symplectic characters. Only a few results, mainly due to Fröhlich, are known.

The aim of this section is to describe one of them, which concerns normal extensions  $N$  of  $\mathbb{Q}$  with Galois group  $G$  isomorphic to the quaternion group  $H_8$  of order 8. Such an extension will be called briefly a quaternion field, and we shall restrict ourselves to the case of a tamely ramified extension (i.e. 2 is not ramified in  $N/\mathbb{Q}$ ).

Write  $H_8 = \langle \sigma, \tau \rangle$  with relations  $\sigma^4 = 1$ ,  $\tau^2 = \sigma^2$ ,  $\tau\sigma\tau^{-1} = \sigma^{-1}$ , and imbed  $H_8$  in the field of quaternions by  $\sigma \mapsto i$  and  $\tau \mapsto j$ . Then the reduced trace defines a character  $\chi$ , with values  $\chi(1) = 2$ ,  $\chi(\sigma^2) = -2$  and  $\chi(s) = 0$  for  $s \neq 1, \sigma^2$ . This character is the unique irreducible character of degree 2 of  $H_8$ . We write  $W_N$  or  $W$

for the Artin root number  $W(\chi)$ .

Since  $N/\mathbb{Q}$  is tamely ramified, the ring  $O_N$  of integers of  $N$  is a projective module over  $\mathbb{Z}[G]$ . Now, the projective class group of  $\mathbb{Z}[H_g]$  is of order 2 (see below). We define an invariant  $U_N$  (or simply  $U$ ) of  $N$  by putting  $U_N = +1$  or  $-1$  according to whether  $O_N$  has a trivial image in this group or not.

Theorem 1 (Fröhlich) -  $W_N = U_N$ .

We shall define in a quite natural way a local invariant  $U_{N,v}$  (or  $U_v$ ) for every place  $v$  of  $\mathbb{Q}$ , with  $U_v = 1$  almost everywhere and  $U = \prod_v U_v$ . Let  $W_{N,v}$  (or  $W_v$ ) be the local root number  $W(\chi_v)$ . Theorem 1. will be a consequence of the following local result we are going to prove.

Theorem 2 -  $W_{N,v} = U_{N,v}$  for every place  $v$  of  $\mathbb{Q}$ .

For the details omitted in the proofs, the reader is referred to [M] and [F].

## §1. $\mathbb{Z}[G]$ -modules

Let  $M$  be a projective  $\mathbb{Z}[G]$ -module. Assume  $M$  is of

rank 1 (i.e.  $\mathbb{Q} \otimes_{\mathbb{Z}} M$  is free with one generator over  $\mathbb{Q}[G]$ ), and define  $M' = \{x \in M \mid x = \sigma^2 x\}$  and  $M'' = \{x \in N \mid x + \sigma^2 x = 0\}$ . Then,  $M'$  (resp.  $M''$ ) can be given a structure of projective module over  $\mathbb{Z}' = \mathbb{Z}[G]/(1 - \sigma^2)$  (resp.  $\mathbb{Z}'' = \mathbb{Z}[G]/(1 + \sigma^2)$ ). Let  $g = G/\{1, \sigma^2\}$ . Then  $g$  is isomorphic to Klein's four group, and  $\mathbb{Z}'$  is isomorphic to  $\mathbb{Z}[g]$ , whereas  $\mathbb{Z}''$  is isomorphic to the ring  $\mathbb{Z}[1, i, j, k]$  of integral quaternions. For both the rings  $\mathbb{Z}'$  and  $\mathbb{Z}''$ , every projective module is free. Let now  $\Phi$  (resp.  $\Psi$ ) be a basis for  $M'$  over  $\mathbb{Z}'$  (resp. for  $M''$  over  $\mathbb{Z}''$ ). It is easily verified that  $\Phi$  and  $\Psi$  are well defined up to the sign and the conjugacy by an element of  $G$ . The following proposition is easy.

Proposition 3     The bases  $\Phi$  and  $\Psi$  can be chosen in such a way that one of the following congruences holds:

- a)             $\Phi \equiv \Psi \pmod{2M}$
- b)             $\Phi \equiv \Phi\Psi + \tau\Psi + \sigma\tau\Phi \pmod{2M}.$

Moreover, for a given module  $M$ , only one of the congruences a) or b) is possible, and  $M$  is free if and only if a) holds.

Proposition 3 implies that there are exactly 2

isomorphism classes of rank 1 projective  $\mathbb{Z}[G]$ -modules. But it can be proved for the particular group  $H_8$  that given a free module  $F$  and a projective module  $P$  over  $\mathbb{Z}[H_8]$ , then  $P \oplus F$  is free if and only if  $P$  is (cf. [M], §2). Hence, the projective class group of  $\mathbb{Z}[G]$  is of order 2, and we identify this group with  $\{-1, +1\}$ .

## §2. Quaternion fields

A quaternion field contains three quadratic subfields  $k_1, k_2, k_3$  with respective discriminants  $d_1, d_2, d_3$ , and a biquadratic subfield  $K$  with discriminant  $d_1 d_2 d_3$ , the compositum of the  $k_i$ 's. We define a positive integer  $D$  by  $D^2 = d_1 d_2 d_3$ . Write  $N = K(\sqrt{M})$  for some  $M \in K$  (one can take  $M = \psi^2$  with the notation of §1 applied to the  $G$ -module  $O_N$ ). Let  $m$  be a square free integer such that  $\mathbb{Q}(\sqrt{m})$  is none of the  $k_i$ 's. By elementary considerations of group theory, one proves that  $N(\sqrt{m})$  contains besides  $N$  a unique quaternion field, say  $N_m$ , and that any quaternion field containing  $K$  is of the form  $N_m$  for some  $m$ . Clearly,  $N_m = K(\sqrt{Mm})$ . Moreover,  $N_m$  is a tamely ramified extension of  $\mathbb{Q}$  if and only if  $m \equiv 1 \pmod{4}$ .

Now let  $p$  be an odd prime number. Since the extensions

$N/k_i$  are cyclic, if  $p$  is ramified in  $K/\mathbb{Q}$ , then every prime above  $p$  in  $K$  is ramified in  $N/K$ . Hence, for every prime factor  $p$  of  $m$ , either  $p$  is ramified in  $K/\mathbb{Q}$  and has ramification index equal to 4 for both the fields  $N$  and  $N_m$ , or  $p$  is not ramified in  $K$  and is ramified in one and only one of the fields  $N, N_m$ , with ramification index 2. Hence, every quaternion field is of the form  $N_m$  for some  $m$ , where  $N$  is a "pure" quaternion field in the sense of [F], namely: every prime number ramified in  $N/\mathbb{Q}$  is ramified in  $K/\mathbb{Q}$ .

We shall need in the sequel to know under what conditions a biquadratic field  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$  can be imbedded in a quaternion field (cf. [F]).

Proposition 4 A necessary and sufficient condition for  $K$  to be a subfield of a quaternion field is that the following condition holds for every place  $p$  of  $\mathbb{Q}$ :

$$\left( \begin{smallmatrix} -1 & d_1 \\ & p \end{smallmatrix} \right) \left( \begin{smallmatrix} -1 & d_2 \\ & p \end{smallmatrix} \right) \left( \begin{smallmatrix} d_1 & d_2 \\ & p \end{smallmatrix} \right) = +1.$$

Note that there is no condition for an unramified  $p$ . If  $p$  is the place at infinity, the above relation simply means that  $K$  must be totally real. If  $p$  splits in some quadratic subfield of  $K$  and is ramified in the others, it

simply means that  $p$  must be congruent to 1 mod 4.

The following proposition can be deduced from proposition 4.

Proposition 5 Let  $m$  be a square free integer. In order that  $k = \mathbb{Q}(\sqrt{m})$  should be a quadratic subfield of a quaternion field, it is necessary and sufficient that  $m$  be positive and not congruent to -1 mod 8.

### §3. The invariant $U_N$

Recall that  $U_N = +1$  if  $O_N$  is a free  $\mathbb{Z}[G]$ -module and  $U_N = -1$  otherwise. Put  $\epsilon(N) = +1$  if  $N$  is totally real and  $\epsilon(N) = -1$  if  $N$  is totally imaginary. Choose  $\Phi$  and  $\psi$  as in §1 for the  $G$ -module  $O_N$ . Then,

$$\psi \equiv \Phi \pmod{2} \Rightarrow \Phi^2 \equiv \psi^2 \pmod{4} \Rightarrow \text{Tr}_{K/\mathbb{Q}}(\Phi^2) \equiv \text{Tr}_{K/\mathbb{Q}}(\psi^2) \pmod{4},$$

whereas

$$\Phi \equiv \sigma\psi + \tau\psi + \tau\sigma\psi \pmod{2} \Rightarrow \text{Tr}_{K/\mathbb{Q}}(\Phi^2) \equiv -\text{Tr}_{K/\mathbb{Q}}(\psi^2) \pmod{4}.$$

$$\text{Hence, } U_N = +1 \Leftrightarrow \text{Tr}_{K/\mathbb{Q}}(\Phi^2) \equiv \text{Tr}_{K/\mathbb{Q}}(\psi^2) \pmod{4}.$$

$$\text{Proposition 6} \quad \text{a) } \text{Tr}_{K/\mathbb{Q}}(\Phi^2) \equiv \frac{1+d_1+d_2+d_3}{4} \pmod{4}.$$



$$b) \operatorname{Tr}_{K/\mathbb{Q}}(\psi^2) \equiv \mathfrak{E}(N) \prod_{\substack{p \text{ ramified} \\ \text{in } N/\mathbb{Q}}} p \pmod{4}.$$

Proof a) We may choose for  $\Phi$  any normal basis of  $K/\mathbb{Q}$ .

Taking  $\Phi = \frac{1+\sqrt{d_1}+\sqrt{d_2}+\sqrt{d_3}}{4}$  gives immediately a).

b) We first remark that  $\psi^2$  is totally positive if  $N$  is real and totally negative otherwise. Hence  $\operatorname{Tr}_{K/\mathbb{Q}}(\psi^2)$  and  $\mathfrak{E}(N)$  have the same sign. To find the ideal of  $\mathbb{Z}$  generated by  $\operatorname{Tr}_{K/\mathbb{Q}}(\psi^2)$ , we compute the discriminant  $D(N/\mathbb{Q})$  of  $N/\mathbb{Q}$  in two ways. On the one hand, write for the bilinear form  $T = \operatorname{Tr}_{N/\mathbb{Q}}(xy)$  the direct sum decomposition  $T = T' \oplus T''$ , where  $T' = \operatorname{Tr}_{K/\mathbb{Q}}(xy)$  on  $N' = K$  and  $T'' = \operatorname{Tr}_{K/\mathbb{Q}}(xy)$  on  $N'' = \{x \in N \mid x + \sigma^2 x = 0\}$ . This gives the formula  $D(N/\mathbb{Q}) = D(K/\mathbb{Q})(\operatorname{Tr}_{K/\mathbb{Q}}(\psi^2))^4$ . On the other hand, we can use ramification groups to compute  $D(N/\mathbb{Q})$ . This gives the formula  $D(N/\mathbb{Q}) = \prod_{\substack{p \text{ ramified} \\ \text{in } N/\mathbb{Q}}} p^4 \prod_{\substack{p \text{ ramified} \\ \text{in } K/\mathbb{Q}}} p^2$ , and b) is proved.

We identify now  $(\mathbb{Z}/4\mathbb{Z})^*$  with  $\{-1, +1\}$ , and write  $\alpha_N$  or  $\alpha$  for the image  $\operatorname{Tr}_{K/\mathbb{Q}}(\Phi^2)$  and  $\beta_N$  or  $\beta$  for the image of  $\operatorname{Tr}_{K/\mathbb{Q}}(\psi^2)$  in  $\{-1, +1\}$ . Hence,  $U_N = \alpha_N \beta_N$ .

There is quite a natural decomposition of  $\beta$  as a product

of local terms  $\beta_{N,v} = \beta_v$ , namely:

$$\beta_\infty = \xi(N)$$

$$\beta_p = 1 \text{ if } p \text{ is unramified}$$

$$\beta_p = \text{image of } p \bmod 4 = (-1)^{(p-1)/2} \text{ if } p \text{ is ramified.}$$

$$\text{Then, } \beta_v = 1 \text{ almost everywhere, and } \beta = \prod_v \beta_v.$$

It is less obvious to find what to choose for the  $\alpha_v$ 's.

We use a remark of Fröhlich (cf. [F], §7):  $\frac{1+d_1+d_2+d_3}{4} \equiv \left(\frac{2}{D}\right) \bmod 4$ , where  $D^2$  is the discriminant of  $K/\mathbb{Q}$ . We now define the  $\alpha_v$ 's:

$$\alpha_v = +1 \text{ if } v \text{ is not ramified in } K/\mathbb{Q} \text{ (in particular,}$$

$$\alpha_\infty = +1)$$

$$\alpha_p = \left(\frac{2}{p}\right) \text{ for a finite prime } p \text{ ramified in } K/\mathbb{Q}.$$

Then,  $\alpha_v = +1$  almost everywhere, and  $\alpha = \prod_v \alpha_v$ . Moreover,  $\alpha_v$  depends only on the field  $K$ .

We now define local terms for  $U_N$  by  $U_{N,v} = U_v = \alpha_v \beta_v$ . Then,  $U_v = +1$  almost everywhere and  $U = \prod_v U_v$ .

#### §4. Some computations of the invariant $U_N$

Let  $p$  be a prime number. Write  $p' = (-1)^{(p-1)/2} p$ , and assume that  $\mathbb{Q}(\sqrt{p'})$  is not one of the fields  $k_i$ . Given a quaternion field  $N$ , we compare the local invariants of  $N$  and  $N' = N_p$ . The proof of the following proposition is obvious

from the definition of the  $\alpha_v$ 's and  $\beta_v$ 's.

Proposition 7

- (i)  $\beta_{N',\infty} = (-1)^{(p-1)/2} \beta_{N,\infty}$
- (ii)  $\beta_{N',p} = (-1)^{(p-1)/2} \beta_{N,p}$  if  $p$  is unramified  
in  $K/\mathbb{Q}$
- (iii)  $\beta_{N',q} = \beta_{N,q}$  otherwise
- (iv)  $\alpha_{N',v} = \alpha_{N,v}$  for all  $v$ .

Corollary 8

$$U_{N'} = U_N \text{ if } p \text{ is unramified in } K/\mathbb{Q}$$

$$U_{N'} = (-1)^{(p-1)/2} U_N \text{ otherwise.}$$

Corollary 9 Let  $\Delta$  be the discriminant of a quaternion field containing a biquadratic field  $K$  such that at least one prime number  $p \equiv 3 \pmod{4}$  is ramified in  $K$ . Then, exactly half of the quaternion fields with discriminant  $\Delta$  have invariant

$$U_N = +1.$$

Corollary 10 Let  $K$  be a biquadratic field such that every prime number ramified in  $K/\mathbb{Q}$  is congruent to  $1 \pmod{4}$ . Then

the quaternion fields  $N$  containing  $K$ , if any, have the same invariant  $U_N$ .

Remark Let us call this invariant  $U_K$ . Using Dirichlet's theorem on primes in arithmetic progressions together with propositions 4 and 5, it is easy to show that there exist infinitely many fields  $K$  with  $U_K = +1$  and infinitely many fields  $K$  with  $U_K = -1$ .

#### §5. Proof of theorem 2.

We must verify for every place  $v$  of  $\mathbb{Q}$  the equality

$$U_{N,v} = W_{N,v}.$$

(i)  $v = \infty$ . If  $N$  is real, then  $\alpha_v = \beta_v = W_v = +1$ . If  $N$  is imaginary, then  $\alpha_v = +1$ ,  $\beta_v = -1$ , hence,  $U_v = -1$ . Now, the only possible choice for a real Frobenius substitution is  $\sigma_v = \sigma^2$ . Hence,

$$n(\chi, v) = \frac{\chi(1) - \chi(\sigma^2)}{2} = 2 \text{ and } W_v = i^{-n(\chi, v)} = -1.$$

We now consider the case of a finite prime  $p$ . Let  $G_p$  be the local Galois group. If  $p$  splits in at least one quadratic subfield of  $N$ , then  $G_p$  is cyclic of order 1, 2 or 4. If  $p$  does not split in  $K$ , then  $p$  is ramified in  $K/\mathbb{Q}$ . Hence,  $p$  is odd,  $G_p = G$  and the inertia group  $I_p$  is

cyclic of order 4. Let  $\chi_p$  be the restriction of  $\chi$  to  $G_p$ .

(ii)  $G_p$  is cyclic. Then,  $\chi_p = \phi_p + \bar{\phi}_p$ , where  $\phi_p$  is a character of  $G_p$  of order equal to that of  $G_p$ . We thus have

$$W_p = W(\chi_p) = \phi_p(-1).$$

If  $I_p = \{1\}$ , then  $\phi_p$  is unramified. Hence,

$$W_p = \phi_p(-1) = +1 = U_p.$$

If  $I_p$  is of order 2, then the restriction of  $\phi_p$  to the group of  $p$ -adic units is the quadratic character  $x \mapsto \left(\frac{x}{p}\right)$ .

Hence,  $W_p = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = U_p$  since  $\alpha_p = 1$  and

$$\beta_p = (-1)^{(p-1)/2}.$$

If  $I_p = G_p$ , then the restriction of  $\phi$  to the group of  $p$ -adic units is a biquadratic character. Hence,  $p \equiv 1$

mod 4 and  $W_p = \phi_p(-1) = (-1)^{(p-1)/4}$ . But  $\alpha_p = 1$  and

$\beta_p = \left(\frac{2}{p}\right)$ . Since  $p \equiv 1 \pmod{4}$ ,  $\left(\frac{2}{p}\right) = (-1)^{(p-1)/4}$  and

$$W_p = U_p.$$

(iii)  $G_p = G$ . Let  $k_p$  be a quadratic subfield of the completion  $N_p$  of  $N$ , let  $H = \text{Gal}(N_p/k_p)$ , and let  $\phi_p$  be a character of  $H$  of order 4.

Then,  $\chi_p = \phi_p^*$ , the character of  $G$  induced by  $\phi_p$ . Let  $\epsilon_p$  be the character of  $G$  lifted from the non trivial character of  $G/H$ . Then,  $1^* = 1 + \epsilon_p$ .

Hence,  $W((\chi_p - 1)^*) = W(\phi_p - 1)$ , and therefore

$W(\chi_p) = W(\phi_p) W(\epsilon_p)$ . Take for  $k_p$  the field

$\mathbb{Q}_p(\sqrt{(p-1)/2})$ . Since  $\mathbb{Q}(\sqrt{(p-1)/2})/\mathbb{Q}$  is ramified only at  $p$ ,  $W_p(\epsilon_p) W_\infty(\epsilon_p) = +1$ . Hence,  $W(\epsilon_p) = +1$  for  $p \equiv 1 \pmod{4}$  and  $W(\epsilon_p) = +i$  for  $p \equiv 3 \pmod{4}$ , a result known to Gauss! We thus have  $W(\epsilon_p)^2 = (-1)^{(p-1)/2} = \beta_p$ . Now, an easy computation shows that the transfer  $\text{Ver}_G^H$  is not trivial.\* This implies that the restriction of  $\phi_p$  to  $\mathbb{Q}_p^*$  is equal to  $\epsilon_p$ . Since  $\alpha_p = \left(\frac{2}{p}\right) = \phi_p(2)$ , theorem 2 is a consequence of the following lemma.

Lemma 11 (Fröhlich, Queyrut) - Let  $K$  be a finite extension of a  $p$ -adic field. Let  $\epsilon$  be a character of  $K^*$  of order 2 corresponding to a quadratic extension  $E$  of  $K$ . Let  $\phi$  be a character of  $E^*$  whose restriction to  $K^*$  is  $\epsilon$ . Assume that both  $\phi$  and  $\epsilon$  are ramified and tamely ramified. Then  $W(\phi) = \phi(2) W(\epsilon)$ .

Proof Let  $v_K, v_E$  be the valuations of  $K, E$  respectively. Since  $\phi$  and  $\epsilon$  are ramified and tamely ramified,

$$v_K(\phi(\epsilon)) = v_E(\phi(\phi)) = 1.$$

With the notation of [M1] II, §2, we have the formulae

---

\*Footnote: see Exercise 7.

$$W(\phi) = \frac{1}{\sqrt{N(f(\phi))}} \tau(\bar{\phi}) \quad \text{and} \quad W(\epsilon) = \frac{1}{\sqrt{N(f(\epsilon))}} \tau(\bar{\epsilon}),$$

with :

$$\tau(\phi) = \sum_{x \in U_E/U_E^1} \phi\left(\frac{x}{c}\right) \psi_E\left(\frac{x}{c}\right) \quad \text{and} \quad \tau(\epsilon) = \sum_{x \in U_K/U_K^1} \epsilon\left(\frac{x}{d}\right) \psi_K\left(\frac{x}{d}\right),$$

where  $c$  generates  $\mathcal{D}_{E/\mathbb{Q}_p} f(\phi)$  and  $d$  generates  $\mathcal{D}_{K/\mathbb{Q}_p} f(\epsilon)$ .

Now,  $v_E(\mathcal{D}_{E/K}) = 1$ . Hence,  $v_E(\mathcal{D}_{E/\mathbb{Q}_p}) = 1 + v_E(\mathcal{D}_{K/\mathbb{Q}_p}) = 1 + 2 v_K(\mathcal{D}_{K/\mathbb{Q}_p})$ , and  $v_E(c) = 2v_K(d)$ . We can therefore choose  $c = d \in K$ . Since  $E/K$  is totally ramified, the inclusion  $K^* \subset E^*$  induces an isomorphism  $U_K/U_K^1 \rightarrow U_E/U_E^1$ . We can therefore choose the  $x$ 's in  $U_K$  to compute  $\tau(\phi)$ . For such a choice for  $c$  and  $x$ ,  $\psi_E\left(\frac{x}{c}\right) = \psi_K\left(\frac{2x}{c}\right)$ . Hence,

$$\tau(\phi) = \bar{\phi}(2) \sum_{x \in U_K/U_K^1} \phi\left(\frac{2x}{d}\right) \psi_K\left(\frac{2x}{d}\right) = \bar{\phi}(2) \tau(\epsilon).$$

Since the conductors  $f(\phi)$  and  $f(\epsilon)$  have the same absolute norm,  $W(\phi) = \phi(2) W(\epsilon)$ ,

Q.E.D.

#### REFERENCES

- [F] A. Fröhlich - Artin Root Numbers and Normal Integral Bases for Quaternion Fields, Invent. Math., 17 (1972), 143-166.



- [M] J. Martinet, Modules sur l'algèbre du groupe quaternionien, Ann. Sci. E.N.S., 4 (1971), 399-408.
- [M1] J. Martinet, Character theory and Artin L-functions, Durham Symposium.

## Un contre-exemple à une conjecture de J. Martinet

Jean Cougnard

Soit  $N/\mathbb{Q}$  une extension galoisienne de groupe de Galois  $G$  ; on note  $O_N$  la clôture intégrale de  $\mathbb{Z}$  dans  $N$ ,  $\mathcal{D}$  un ordre maximal de  $\mathbb{Q}[G]$ . On considère le  $\mathcal{D}$ -module  $\mathcal{D}O_N$  ; J. Martinet a conjecturé que  $\mathcal{D}O_N$  est  $\mathcal{D}$ -stablement libre. A Fröhlich a montré que cette conjecture était vérifiée quel que soit  $G$  pourvu que l'extension  $N/\mathbb{Q}$  soit modérément ramifiée ([6], [6a]). On sait qu'elle est également vraie lorsque  $G$  est un  $p$ -groupe, indépendamment de la ramification [4]. Le but de cet exposé est de donner un contre-exemple à la conjecture.

### §.I. Groupes non abéliens d'ordre $pq$

Soient  $G$  un groupe et  $\chi$  un caractère de  $G$  ; la fonction  $\chi$  se prolonge par linéarité en une fonction sur  $\mathbb{Q}[G]$  que l'on note encore  $\chi$ . Lorsque le caractère est absolument irréductible, il existe un et un seul facteur simple de  $\mathbb{Q}[G]$  sur lequel la fonction  $\chi$  n'est pas identiquement nulle ;

ce facteur simple est appelé facteur simple associé à  $\chi$  [5].

On suppose désormais que  $G$  est un groupe non abélien d'ordre  $pq$  ( $p$  et  $q$  premiers avec  $q \neq 2$ ); il est engendré par deux éléments  $\sigma$  et  $\tau$  vérifiant les relations:

$$\sigma^p = \tau^q = 1, \quad \tau\sigma\tau^{-1} = \sigma^r \quad \text{où} \quad r \not\equiv 1(p), \quad r^q \equiv 1(p),$$

ce qui implique  $p \equiv 1(q)$ . On note  $H$  (resp.  $g$ ) le sous-groupe de  $G$  engendré par  $\sigma$  (resp.  $\tau$ ). Le sous-groupe  $H$  est distingué et l'on note  $\bar{\tau}$  l'image de  $\tau$  dans  $G/H$ .

Le groupe  $G$  possédant trois classes de conjugaison de sous-groupes cycliques, l'algèbre  $\mathbb{Q}[G]$  est produit de trois facteurs simples ([10] cor. 1 au th. 29). Le premier facteur est isomorphe à  $\mathbb{Q}$  et est associé au caractère identité, le second est isomorphe à  $\mathbb{Q}(\omega)$  où  $\omega$  est une racine primitive  $q$ -ème de l'unité et est associé aux caractères de degré 1 non triviaux de  $G$ . On peut démontrer que le troisième facteur est une algèbre de matrices à coefficients dans le sous-corps du  $p$ -ème corps cyclotomique dont le degré sur  $\mathbb{Q}$  est  $\frac{p-1}{q}$  ([3]); ce facteur est associé aux caractères de la forme  $\text{Ind}_H^G \xi$  où  $\xi$  est un caractère de degré 1 de  $H$ , non trivial.

Un ordre maximal de  $\mathbb{Q}[G]$  contenant  $\mathbb{Z}[G]$  est donc de la

forme  $\mathcal{D} = \mathbb{Z} \times \mathbb{Z}[\omega] \times \mathcal{D}'$  où  $\mathcal{D}'$  est un ordre maximal du troisième facteur simple. Rappelons la proposition suivante:

Proposition I.1. Soient  $e_i$  ( $i = 1, 2, 3$ ) les idempotents du centre tels que  $e_i \mathbb{Q}[G]$  soit le  $i$ -ème facteur simple et soit  $M$  un  $\mathcal{D}$ -module sans torsion. Le  $\mathcal{D}$ -module  $M$  est stablement libre si, et seulement si, pour chaque  $i$ ,  $e_i M$  est  $e_i \mathcal{D}$ -stablement libre.

## §.II. Extensions et résolvantes de Lagrange

Soit  $N/\mathbb{Q}$  une extension galoisienne, non abélienne, de degré  $pq$ . On note  $k$  (resp.  $K$ ) le sous-corps de  $N$  invariant par le sous-groupe  $H$  (resp.  $g$ ). Soit  $\chi$  un caractère de  $G$  de degré 1; un tel caractère est trivial sur  $H$  et définit un caractère  $\chi'$  du groupe de Galois de  $k/\mathbb{Q}$ .

Definition II.1. On définit des résolvantes de Lagrange par:

a) pour  $\theta \in N$  et  $\chi$  caractère de degré 1 de  $G$ :

$$\langle \theta, \chi \rangle = \sum_{g \in G} g(\theta) \chi(g^{-1}) \quad ,$$

b) pour  $\theta \in k$  et  $\chi$  caractère de degré 1 de  $G$ :

$$(\theta, \chi) = \sum_{i=1}^q \tau^{-i}(\theta) \chi'(\tau^{-i}).$$

Proposition II.1. On a la relation  $\langle \theta, \chi \rangle = (T_{N/k}(\theta), \chi)$ .

Démonstration On applique les définitions en remarquant que  $\chi$  restreint à  $H$  est le caractère trivial.

Rappelons maintenant les propriétés élémentaires des résolvantes de Lagrange. L'élément  $\langle \theta, \chi \rangle$  appartient à  $N(\omega)$ . Comme les extensions  $N/\mathbb{Q}$  et  $\mathbb{Q}(\omega)/\mathbb{Q}$  sont linéairement disjointes sur  $\mathbb{Q}$ , on a  $\text{Gal}(N(\omega)/\mathbb{Q}) \simeq \text{Gal}(N(\omega)/N) \times \text{Gal}(N(\omega)/\mathbb{Q}(\omega))$ . Pour  $1 \leq i < q$  on note  $s_i$  le  $N$ -automorphisme de  $N(\omega)$  tel que  $s_i(\omega) = \omega^i$  et on identifie les éléments de  $\text{Gal}(N(\omega)/\mathbb{Q}(\omega))$  avec leur restriction à  $N$ . On peut alors énoncer:

Proposition II.2. a) Quels que soient  $\theta \in N$ ,  $\chi$  caractère de degré 1 de  $G$  et  $g \in G$ ,

$$g(\langle \theta, \chi \rangle) = \langle g\theta, \chi \rangle = \chi(g) \langle \theta, \chi \rangle.$$

b) Quels que soient  $\theta \in N$ ,  $\chi$  caractère de degré 1 de  $G$  et  $1 \leq i < q$   $s_i(\langle \theta, \chi \rangle) = \langle \theta, \chi^i \rangle$ .

On en déduit immédiatement:

Corollaire 1.      a)    Quels que soient  $\theta \in N$  et  $\chi$  caractère de degré 1 de  $G$ ,

$$\langle \theta, \chi \rangle^q \in \mathbb{Q}(\omega).$$

b)    Quels que soient  $\theta \in N$ ,  $\chi$  et  $\chi'$  caractères de degré 1 de  $G$  tels que

$$\langle \theta, \chi\chi' \rangle \neq 0, \quad \frac{\langle \theta, \chi \rangle \langle \theta, \chi' \rangle}{\langle \theta, \chi\chi' \rangle} \in \mathbb{Q}(\omega)$$

en particulier si

$$\langle \theta, \chi \rangle \neq 0 \quad \beta_i(\chi) = \frac{\langle \theta, \chi \rangle^i}{\langle \theta, \chi \rangle^i} \in \mathbb{Q}(\omega).$$

c)    Quels que soient  $\theta$  et  $\theta' \in N$ ,  $\chi$  caractère de degré 1 de  $G$  tels que  $\langle \theta, \chi \rangle \neq 0$ , l'élément  $\frac{\langle \theta', \chi \rangle}{\langle \theta, \chi \rangle}$  appartient à  $\mathbb{Q}(\omega)$ .

On peut démontrer aisément que si  $\theta$  forme avec ses conjugués une base normale de  $N/\mathbb{Q}$ , alors quel que soit le caractère  $\chi$  de degré 1 de  $G$ ,  $\langle \theta, \chi \rangle \neq 0$ .

On se fixe un élément  $\theta_0$  vérifiant la condition ci-dessus, et un caractère  $\chi$  de degré 1 de  $G$ , non trivial.

Définition II.2. On définit l'application  $f$  (resp.  $f'$ ) de  $N$  (resp.  $k$ ) dans  $\mathbb{Q}(\omega)$  par  $f(\theta) = \frac{\langle \theta, \chi \rangle}{\langle \theta_o, \chi \rangle}$  (resp.  $f'(\theta) = \frac{(\theta, \chi)}{(T_{N/k} \theta_o, \chi)}$ ).

On peut énoncer:

Proposition II.3. L'application  $f$  (resp.  $f'$ ) est une surjection de  $N$  (resp.  $k$ ) sur  $\mathbb{Q}(\omega)$ . Etant donné  $x \in \mathbb{Q}(\omega)$ , l'élément  $\theta = \frac{1}{q} T_{k(\omega)/k}(x(T_{N/k} \theta_o, \chi))$  est tel que  $f'(\theta) = x$ .

Démonstration. L'extension  $N/k$  étant séparable, la trace  $T_{N/k}$  est surjective, il suffit donc, d'après la proposition II.1., de vérifier la surjectivité de  $f'$ . La deuxième partie de la proposition, que l'on vérifie par un calcul élémentaire, prouve cette surjectivité.

On munit  $\mathbb{Q}(\omega)$  d'une structure de  $\mathbb{Q}[G]$ -module en posant pour tout  $y$  de  $\mathbb{Q}[G]$  et tout  $\alpha$  de  $\mathbb{Q}(\omega)$

$$y * \alpha = \chi(y) \alpha .$$

La partie a) de la proposition II.2. et la proposition II.3. montrent que  $f$  est un homomorphisme surjectif du  $\mathbb{Q}[G]$ -module  $N$  sur le  $\mathbb{Q}[G]$ -module  $\mathbb{Q}(\omega)$ . Or  $\mathbb{Q}(\omega)$  est isomorphe à  $e_2 \mathbb{Q}[G]$  et  $\mathbb{Q}[G]$  est semi-simple. On en déduit que pour tout ordre  $\mathcal{O}'$  de  $\mathbb{Q}[G]$  et tout  $\mathcal{O}'$ -module  $M$



inclus dans  $N$ ,  $f(M)$  est  $e_2 \mathcal{D}'$  isomorphe à  $e_2 M$ . On constate par ailleurs que si  $\mathcal{D}$  est un ordre maximal contenant  $\mathbb{Z}[G]$ , on a  $e_2 \mathcal{D} = e_2 \mathbb{Z}[G] \simeq \mathbb{Z}[\omega]$ . Il s'ensuit que  $f(\mathcal{D} O_N) \simeq e_2 (\mathcal{D} O_N) = e_2 \mathcal{D} e_2 O_N \simeq \mathbb{Z}[\omega] f(O_N) = f(O_N)$ .

Pour donner un contre-exemple à la conjecture, il suffit de trouver une extension  $N/\mathbb{Q}$  non abélienne de degré  $pq$  telle que  $f(O_N) = f'(T_{N/k} O_N)$  ne soit pas  $\mathbb{Z}[\omega]$ -libre.

Remarquons tout de suite:

Proposition II.4. Il existe un entier  $m$  tel que

$T_{N/k}(O_N) = P^m$  où  $P$  désigne le produit des idéaux premiers de  $O_k$  (clôture intégrale de  $\mathbb{Z}$  dans  $k$ ) au-dessus de  $p$ .

Démonstration. Il suffit de localiser aux places différentes de  $p$  et d'utiliser la surjectivité de la trace du localisé de  $O_N$  dans le localisé de  $O_k$  (à cause de la ramification modérée).

La valeur de  $m$  sera déterminée ultérieurement.

### §.III. Décomposition des résolvantes de Lagrange

L'idéal principal de  $\mathbb{Q}(\omega)$  engendré par  $\langle \theta_0, \chi \rangle^q$  se décompose de façon unique sous la forme:

$$\alpha(\chi) = (\langle \theta_o, \chi \rangle^q) = R(\chi)^q \prod_{i=1}^{q-1} A_i(\chi)^i$$

où  $R(\chi)$  est un idéal fractionnaire et les  $A_i(\chi)$  des idéaux entiers, premiers entre eux deux à deux, sans facteur carré.

Notation. Pour tout entier  $n$  premier à  $q$ ,  $[n]$  désigne l'entier vérifiant  $0 < [n] < q$  et  $n \equiv [n] \pmod{q}$ .

Lemme III.1. Quels que soient  $i, j$  tels que  $1 \leq i, j < q$ , on a:

$$A_{[i \ j]}(\chi^i) = A_j(\chi) \quad .$$

Démonstration. On utilise le corollaire 1, b) à la proposition II.2. qui nous donne  $\alpha(\chi^i) = \alpha(\chi)^i \beta_i(\chi)^q$ . On décompose les deux membres sous la forme indiquée ci-dessus. La décomposition étant unique il suffit de comparer les deux membres pour obtenir le lemme.

Lemme III.2. Quels que soient les entiers  $i, j$  vérifiant  $1 \leq i, j < q$ , on a:

$$s_j(A_i(\chi)) = A_i(\chi^j).$$

Démonstration. On utilise la proposition II.2.b et on procède comme dans le lemme 1.

Notation. Pour tout entier  $i$  premier à  $q$ , on note  $i^*$  l'entier vérifiant les conditions  $1 \leq i^* < q$ ,  $ii^* \equiv 1(q)$ .

Lemme III.3. On peut écrire  $\alpha(\chi) = R(\chi)^q \prod_{j=1}^{q-1} s_j(A_1(\chi))^{j^*}$ .

Démonstration. Cela résulte immédiatement des lemmes III.1. et III.2.

Remarque: A l'aide de la décomposition du lemme III.3., de la théorie de Kummer et des considérations évidentes sur les indices de ramification, on constate qu'un idéal premier  $(\ell) \nmid q$  de  $\mathbb{Z}$  est ramifié dans  $k/\mathbb{Q}$  si et seulement si il existe un idéal premier  $L$  de  $\mathbb{Z}[\omega]$  au-dessus de  $(\ell)$  divisant  $A_1(\chi)$ .

Définition III.1. En suivant la terminologie de [1], on appelle idéal essentiel de  $\mathbb{Q}(\omega)$  un idéal fractionnaire principal  $I$  tel que, quel que soit  $j$ ,  $1 \leq j < q$ ,  $s_j(I) = I^j M_j^q$  où  $M_j$  est principal.

On remarque que les idéaux essentiels forment un sous-groupe du groupe des idéaux fractionnaires.

Lemme III.4. Tout idéal fractionnaire de  $\mathbb{Q}(\omega)$  de la forme  $\prod_{i=1}^{q-1} s_j(B)^j$ , où  $B$  est un idéal quelconque, est un idéal essentiel.

Lemme III.5. Soit  $I$  un idéal, fractionnaire de  $\mathbb{Q}(\omega)$ , tel que  $I^q$  soit essentiel, alors  $I$  est principal.

On trouvera une démonstration des lemmes III.4. et III.5. dans [1].

Proposition III.1. L'image  $f'(O_k)$  est un idéal fractionnaire principal de  $\mathbb{Q}(\omega)$ .

Démonstration. Les lemmes III.3., III. 4. et III.5.

montrent que  $R(\chi)$  est un idéal principal. Par ailleurs, si  $\theta \in O_k$ ,  $(\theta, \chi)$  est un entier, donc  $(T_{N/k}^{\theta} O, \chi) f'(\theta)$  est un

entier d'où l'on déduit que l'idéal

$(f'(\theta) R(\chi))^q \prod_{j=1}^{q-1} s_j(A_1(\chi))^j$  est entier. Ceci montre que

$f'(\theta) \in R(\chi)^{-1}$ . Inversement, la deuxième partie de la proposition II.3. montre que  $f'(O_k) \supset q R(\chi)^{-1}$ . On a donc la double inclusion  $q R(\chi)^{-1} \subset f'(O_k) \subset R(\chi)^{-1}$ . De plus  $f'(O_k)$  est stable par la multiplication par  $\omega^i = \chi(\tau^i)$  et par la multiplication par les éléments de  $\mathbb{Z}$ . Il s'ensuit que  $f'(O_k)$  est un idéal fractionnaire. On termine la démonstration en remarquant que  $(q)$  est une puissance d'un idéal premier principal de  $\mathbb{Z}[\omega]$ .

Supposons désormais que  $N/\mathbb{Q}$  soit totalement ramifiée en  $p$ , que  $k/\mathbb{Q}$  soit non ramifiée en  $q$  et que l'entier  $m$  vérifie  $0 < m < q$ . On peut alors appliquer un théorème de S. Ullom (théorème 1 de [11]). On a alors, en notant  $P_1$  l'idéal premier dans  $\mathbb{Q}(\omega)$  au-dessus de  $(p)$  et divisant  $A_1(\chi)$  :

$$f'(P^m) = f'(O_k) P_1^{u(m)}$$

où  $u(m)$  est l'élément de  $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})]$  défini par

$$u(m) = \sum_{j=1}^{q-1} c_j(m) s_j^{-1}$$

avec  $c_j(m) = 1 + \left[ \frac{m-j-1}{q} \right]$ ,  $[x]$  désignant le plus grand entier inférieur ou égal à  $x$ .

Remarque 1. Si  $p = 47$ ,  $q = 23$ , l'idéal  $P_1$  n'est pas principal. En effet, s'il l'était, sa norme dans  $\mathbb{Q}(\sqrt{-23})$  sous corps quadratique de  $\mathbb{Q}(\omega)$  serait un idéal principal. L'équation  $N_{\mathbb{Q}(\sqrt{-23})/\mathbb{Q}}(a \frac{1+\sqrt{-23}}{2} + b \frac{1+\sqrt{-23}}{2}) = 47$  aurait des solutions entières. On vérifie rapidement que ce n'est pas le cas.

Remarque 2. Si pour  $p = 47$ ,  $q = 23$ , on peut avoir  $m = 2$ ; on a  $c_j(m) = 0$  sauf pour  $j = 1$  où  $c_j(m) = 1$ , et alors  $u(m) = \text{id}$  et  $f(O_N) = f'(O_k) P_1$ , qui n'est pas un idéal principal d'après la proposition III.1. et la remarque 1. On aura alors le contre-exemple recherché d'après la discussion de la fin du paragraphe II.

#### §.IV. Construction de l'extension

Tout d'abord déterminons l'entier  $m$  en fonction de la ramification de  $N/\mathbb{Q}$  en  $p$ . Puisque  $N/\mathbb{Q}$  est totalement ramifiée en  $p$ .  $N/k$  est sauvagement ramifiée. Le degré  $N/k$  est premier; on en déduit que les sauts de ramification en notation supérieure et inférieure coïncident. La suite des groupes de ramification de  $P$  dans  $N/k$  est donc

$$H = H_0 = H^0 = \dots = H^t = H_t \supset H_{t+1} = \{1\}.$$

On a un premier renseignement sur la valeur de  $t$  (cf. [8]) : puisque l'indice de ramification absolu de  $P$  est  $q$ , on a  $1 \leq t \leq \left[ \frac{pq}{p-1} \right]$ . Comme nous allons nous intéresser au cas  $q = 23$ , on peut supposer  $p \neq 3$ , donc  $\left[ \frac{pq}{p-1} \right] = q$ . Un raisonnement analogue à celui de ([8] prop. III.4.) montre que l'on a  $1 \leq t < q$ .

Proposition IV.1. L'entier  $m$  est égal à  $t$ .

Démonstration. On applique le lemme 4 du chapitre V de [9] et l'on a  $m = \left[ \frac{(t+1)(p-1)}{p} \right] = \left[ t+1 - \frac{t+1}{p} \right]$ . Les inégalités  $2 \leq t+1 \leq q < p$  entraînent le résultat.

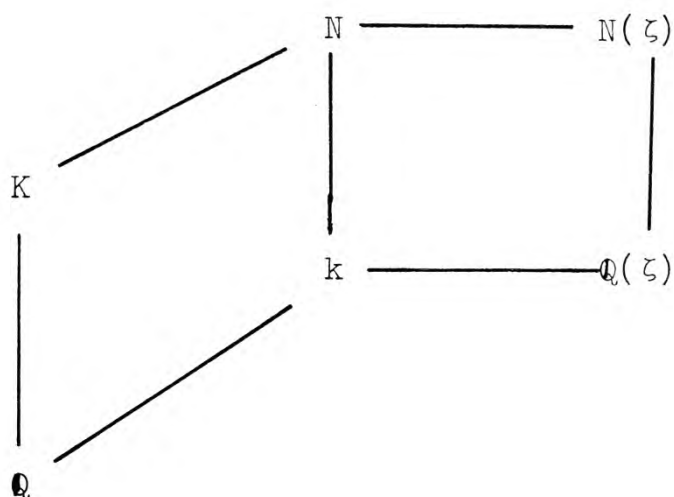
Remarquons que la condition  $m < q$  du théorème I de [11] est d'ores et déjà vérifiée.

La relation  $p \equiv 1 \pmod{q}$  montre que le  $p$ -ième corps cyclotomique contient un et un seul sous corps de degré  $q$  sur  $\mathbb{Q}$ . C'est ce corps que nous choisirons comme corps  $k$ . La condition  $k/\mathbb{Q}$  non ramifiée en  $q$  du théorème I de [11] est alors automatiquement vérifiée.

Supposons construite une extension non abélienne  $N$  de  $\mathbb{Q}$ , de degré  $pq$  contenant le corps  $k$  défini ci-dessus.



Soit  $\zeta$  une racine primitive  $p$ -ème de l'unité. On a alors le diagramme ci-dessous.



Les extensions  $K/\mathbb{Q}$  et  $\mathbb{Q}(\zeta)/\mathbb{Q}$  sont linéairement disjointes sur  $\mathbb{Q}$ . Le groupe de Galois de  $N(\zeta)/\mathbb{Q}$  est produit semi-direct de  $\text{Gal}(N(\zeta)/K)$  (qui s'identifie de façon canonique à  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  par le sous-groupe distingué  $\text{Gal}(N(\zeta)/\mathbb{Q}(\zeta))$  (qui est isomorphe à  $\text{Gal}(N/k)$ ). On peut trouver un  $K$ -automorphisme  $\mu_j$  de  $N(\zeta)$  vérifiant  $\mu_j(\zeta) = \zeta^j$  ( $1 < j < p$ ) dont la restriction à  $N$  soit  $\tau$  et qui soit un générateur de  $\text{Gal}(N(\zeta)/K)$ . Le groupe de Galois de  $N(\zeta)/\mathbb{Q}$  est engendré par deux éléments  $\sigma$  et  $\mu_j$  vérifiant:

$$\sigma^p = \mu_j^{p-1} = 1 \quad \mu_j \sigma \mu_j^{-1} = \sigma^r$$

(l'entier  $r$  vérifiant les mêmes conditions qu'au

paragraphe I).

Notation. L'entier  $j$  étant fixé modulo  $p$ , il existe un et un seul entier  $n$ , défini modulo  $q$ , tel que  $r \equiv j^{n(p-1/q)}(p)$ . On définit  $\bar{r}$  par  $1 \leq \bar{r} < p$ ,  $r\bar{r} \equiv 1(p)$ , et  $j'$  par  $1 \leq j' < p$ ,  $j' \equiv j\bar{r}(p)$ .

L'extension  $N(\zeta)/\mathbb{Q}(\zeta)$  est cyclique d'ordre  $p$ , sauvagement ramifiée, elle ne possède qu'un saut de ramification noté  $t'$ .

Proposition IV.2. Les entiers  $t$  et  $t'$  sont liés par la relation  $t = t' \frac{q}{p-1}$ .

Démonstration. Soit  $G' = \text{Gal}(N(\zeta)/k)$ ; la suite des groupes de ramification de  $p$  dans  $N(\zeta)/k$  en numérotation inférieure peut s'écrire:

$$G' = G'_0 \supset H = G'_1 = \dots = G'_{t'} = H_{t'} \supset H_{t'+1} = G'_{t'+1} = \{1\}.$$

On en déduit la fonction  $\phi$  de Herbrandt en  $p$  de l'extension  $N(\zeta)/k$ :

$$\phi(u) = \int_0^u \frac{dv}{[G'_0 : G'_v]} \quad (\text{cf. [9] ch. V}) \text{ et qui vaut :}$$

$$\text{pour } 0 \leq u \leq t' \quad \phi(u) = \frac{uq}{p-1} ;$$

$$\text{pour } u \geq t' \quad \phi(u) = \frac{p-1}{q} (t'(1-p) + pu).$$

La relation entre numérotations supérieures et inférieures

$G'_u = G'^{\phi(u)}$  montre que le dernier saut de ramification

supérieure pour  $p$  dans  $N(\zeta)/k$  vaut  $t' \frac{q}{p-1}$ . Les

propriétés de la numérotation supérieure ([9] ch. V)

montrent que le saut supérieur dans  $N/k$  est  $\frac{t'q}{p-1} = t$  ce qui démontre la proposition.

Le calcul de  $t$  se ramène donc à celui de  $t'$ , lequel peut être effectué par la méthode de Kummer. A cet effet, rappelons les résultats de [2]. Soient  $\xi$  un caractère de degré 1 de  $H$ , et  $\theta_1$  un élément de  $K$  engendrant avec ses

conjugués une base normale de  $N/k$ . Considérons la

résolvante de Lagrange  $[\theta_1, \xi] = \sum_{x=0}^{p-1} \sigma^x(\theta_1) \xi(\sigma^{-x})$ .

L'élément  $[\theta_1, \xi]$  appartient à  $N(\zeta)$ . On constate aisément

que  $[\theta_1, \xi]^p \in \mathbb{Q}(\zeta)$  et que si  $n \frac{p-1}{q} \neq 1(q)$  l'élément

$[\theta_1, \xi]^p$  engendre  $\mathbb{Q}(\zeta)$  et vérifie la relation

$\mu_j([\theta_1, \xi]^p) = ([\theta_1, \xi]^p)^{j'} a^p$  avec  $a$  appartenant à  $\mathbb{Q}(\zeta)^*$ . On

démontre [2] que réciproquement étant donné un élément  $\alpha$  de

$\mathbb{Q}(\zeta)^*$ ,  $\alpha \notin \mathbb{Q}(\zeta)^{*p}$  et vérifiant  $\mu_j(\alpha) = \alpha^{j'} a^p$  alors

$\mathbb{Q}(\zeta) (\sqrt[p]{\alpha})$  contient un sous-corps  $N$  qui est une extension

galoisienne de  $\mathbb{Q}$  contenant  $k$ , dont le groupe de Galois est du type souhaité.

Etant donné un tel élément  $\alpha$ , on peut aisément déterminer l'entier  $t'$ . Pour cela localisons et complétons en  $p$  et supposons que  $\alpha$  soit une unité du localisé. On peut, quitte à multiplier  $\alpha$  par une puissance  $p$ -ième supposer que  $\alpha \in U^{(1)}$  (on utilise la notation habituelle pour la filtration du groupe des unités d'un corps local).

Rappelons la définition et les résultats de [12].

Définition IV.1. Soit  $x \in U$ , on note  $\text{Déf}(x)$  l'entier défini par

$$\text{Déf}(x) = \max(v(x - y^p), y \in U)$$

où  $v$  est la valuation qui prend ici la valeur 1 pour l'élément  $1 - \zeta$ .

Proposition IV.3. Soit  $x \in U$  ; supposons que  $v(x-1) = s$  avec  $0 \leq s < p$  alors  $\text{Déf}(x) = s$ .

Proposition IV.4. Supposons  $x \in U$  et  $1 < \text{Déf}(x) < p$  ; alors, l'extension  $\mathbb{Q}_p(\zeta)(\sqrt[p]{x})$  est cyclique totalement ramifiée avec pour nombre de ramification  $t' = p - \text{Déf}(x)$ .

Application. Nous choisissons  $p = 47$ ,  $q = 23$ , nous voulons  $t = 2$ , donc  $t' = \frac{p-1}{q} t = 4$ . Il faut donc déterminer un élément  $\alpha$  de  $U^{(43)}$  tel que  $s_j(\alpha)/\alpha^{j'}$  soit une puissance  $47^{\text{ème}}$  dans  $\mathbb{Q}_{47}(\zeta)$ .

On écrit  $\alpha = 1 + \sum_{n=43}^{\infty} a_n (1 - \zeta)^n$ ,  $0 \leq a_n < p$ , et

l'on pose  $\alpha_1 = 1 + \sum_{n=43}^{47} a_n (1 - \zeta)^n$ . On remarque que

$\alpha_1^{-1} \in U^{(48)}$ ; or, d'après [9], ch. XIV, prop. 9,  $U^{(48)} = (U^{(2)})^{47}$ . On peut donc se contenter de

rechercher les éléments de la forme  $\alpha_1$ , ces éléments présentant l'avantage d'appartenir à  $\mathbb{Q}(\zeta)$ . On a :

$$\mu_j(\alpha_1) = 1 + \sum_{n=43}^{47} a_n (1 - \zeta^j)^n, \quad \text{d'où :}$$

$$\mu_j(\alpha_1) \alpha_1^{-j'} \equiv (1 + \sum_{n=43}^{47} (1 - \zeta^j)^n) (1 - j' \sum_{n=43}^{47} a_n (1 - \zeta)^n) \pmod{(1 - \zeta)^{48}}$$

$$\equiv \sum_{n=43}^{47} a_n ((1 - \zeta^j)^n - j' (1 - \zeta)^n) \pmod{(1 - \zeta)^{48}},$$

on écrit alors :

$$(1 - \zeta^j)^n \equiv \sum_{k=n}^{47} c_{j,k}^n (1 - \zeta)^k \pmod{(1 - \zeta)^{48}}, \quad \text{où } c_{j,n}^n = j^n,$$

d'où :

$$\begin{aligned}
 \mu_j(\alpha_1) \alpha_1^{-j'} &\equiv 1 + \sum_{n=43}^{47} a_n \left( \sum_{k=n}^{47} c_{j,k}^n (1-\zeta)^k - j' (1-\zeta)^n \right) \\
 &\quad \text{mod } (1-\zeta)^{48} \\
 &\equiv 1 + \sum_{n=43}^{47} \left( \sum_{k=43}^{n-1} a_k c_{j,n}^k + a_n (c_{j,n}^n - j') \right) (1-\zeta)^n \\
 &\quad \text{mod } (1-\zeta)^{48}.
 \end{aligned}$$

Si on trouve des  $a_n$  ( $43 \leq n \leq 47$ ) tels que les coefficients de  $(1-\zeta)^n$  dans la dernière congruence soient nuls, avec  $a_{43} \neq 0$ , on aura un élément  $\alpha_1$  vérifiant les conditions souhaitées. Constatons que l'on peut remplacer les coefficients  $c_{j,n}^k$  par leur reste modulo 47 : ils apparaissent comme facteur de  $(1-\zeta)^{43}$ , et comme  $(47) = (1-\zeta)^{46}$ , le remplacement ne modifie pas la congruence modulo  $(1-\zeta)^{48}$ .

On obtient un système d'équations linéaires dont la matrice associée est triangulaire. On aura une solution avec  $a_{43} \neq 0$  si et seulement si les conditions suivantes sont remplies :

- a)  $c_{j,43}^{43} - j' \equiv 0 \pmod{47}$
- b)  $c_{j,n}^n \not\equiv 0 \pmod{47}$  si  $43 < n$ .

La deuxième condition est toujours vérifiée puisque

$$c_{j,n}^n \equiv j^n \neq 0 \quad (47) .$$

La première condition s'écrit  $j^{43} - j^{1-2n} \equiv 0 \quad (47)$ , soit  $1-2n \equiv 43 \quad (46)$  ce qui impose la valeur  $n = 2$  ! On peut donc énoncer :

Théorème IV.1. Il existe des extensions  $N/\mathbb{Q}$  galoisiennes, non abéliennes, de degré  $47 \times 23$  telles que le  $\mathcal{D}$ -module  $\mathcal{D}O_N$  ne soit pas stablement libre.

Démonstration: Les calculs précédents montrent que l'extension  $\mathbb{Q}_p(\zeta, \sqrt[p]{\alpha_1}) / \mathbb{Q}_p$  possède le groupe de Galois et la ramification souhaités. Considérons l'extension  $\mathbb{Q}(\zeta, \sqrt[p]{\alpha_1}) / \mathbb{Q}$ , elle peut ne pas être galoisienne. Soit  $L$  sa clôture galoisienne,  $L$  est le composé d'un nombre  $b$  de corps qui sont de la forme  $\mathbb{Q}(\zeta, \sqrt[p]{\mu_j^x(\alpha_1)})$ . tous ces corps sont cycliques de degré  $p$  sur  $\mathbb{Q}(\zeta)$  et l'on a  $\text{Gal}(L/\mathbb{Q}(\zeta)) \simeq (\mathbb{Z}/p\mathbb{Z})^b$ . On voit immédiatement que  $\text{Gal}(L/\mathbb{Q}(\zeta))$  est un  $F_p$ -espace vectoriel  $V$  de dimension  $b$ . Le groupe de Galois  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  opère par automorphismes intérieurs sur  $V$ ; or  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  est cyclique d'ordre  $p-1$  et  $F_p$  contient les racines  $(p-1)$  èmes de l'unité. Un



théorème de Brauer permet alors de dire que  $L$  est le composé de  $b$  sous-corps  $L_i$ , chacune des extensions  $L_i/\mathbb{Q}$  étant galoisienne. Par construction  $L/\mathbb{Q}(\zeta)$  est ramifiée en  $p$  donc au moins une des extensions  $L_i/\mathbb{Q}(\zeta)$  est ramifiée en  $p$ . On constate aisément que le localisé en  $p$  de cette extension est le corps  $\mathbb{Q}_p(\zeta, {}^p\sqrt{\alpha_1})$  ce qui montre que cette extension fourni le contre-exemple cherché.

## BIBLIOGRAPHIE

1. A. Chatelet., Idéaux principaux dans les corps circulaires, Colloque du C.N.R.S., Algèbre et théorie des nombres, Paris (1949), 103-106.
2. J. Cougnard., Sur les extension galoisiennes non abéliennes de degré  $pq$  ( $p$  et  $q$  premiers) des rationnels, C.R. Acad. Sc. Paris, t. 274 (1972), 936-939.
3. J. Cougnard, Propriétés galoisiennes des anneaux d'entiers, Thèse, Bordeaux, (1975).
4. J. Cougnard, Propriétés galoisiennes des anneaux d'entiers des  $p$ -extensions (à paraître).
5. J.-M. Fontaine, Sur la décomposition des algèbres de groupes, Ann. Scient. E. N. Sup. 4ème série, t. 4, fasc. 1, (1971), 121-180.
6. A. Fröhlich, Arithmetic and Galois module Structure for tame extensions (à paraître).
- 6a. A. Fröhlich, Galois Module Structure, Durham Symposium.
7. G. Gras, Extensions abéliennes non ramifiées de

degré premier d'un corps quadratique, Thèse de troisième cycle, Grenoble, (1970).

8. J. Martinet, Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre  $2p$ , Ann. Inst. Fourier, XIX, (1969), 1-80.
9. J.-P. Serre, Corps locaux, 2ème édition, Hermann, Paris (1968).
10. J.-P. Serre, Représentations linéaires des groupes finis, 2ème édition, Hermann, Paris (1971).
11. S. Ullom, Integral representations afforded by ambiguous ideals in some abelian extensions, J. Number Theory 6, (1974), 32-49.
12. B.F. Wyman, Wildly ramified gamma extensions, Amer. J. Math. XCI (1969), 135-145.

A Stickelberger Condition on Galois module structure  
for Kummer extensions of Prime degree

Leon R. McCulloh (\*)

- §1 The Main Theorem
- §2 Description of the Class Group
- §3 Calculation of  $\text{cl}(\mathcal{O}_L)$
- §4 The Stickelberger Condition
- §5 Corollaries

If  $L/K$  is a tamely ramified Galois extension of algebraic number fields, with Galois group  $G$ , then one knows that the ring  $\mathcal{O}_L$  of integers of  $L$  is a rank one locally free module over the group ring  $\mathcal{O}_K G$ , where  $\mathcal{O}_K$  is the ring of integers of  $K$ . This fact was first pointed out, but not

---

(\*) Footnote: The author wishes to express his gratitude to King's College, London for the generous hospitality extended to him while the major part of this work was being done.

proved, by E. Noether in [16]; cf. [1, p.22].

The object of this paper is to characterise, in certain circumstances, those stable isomorphism classes of  $O_K G$ -modules which contain the ring of integers of some tamely ramified extension  $L/K$  with  $\text{Gal}(L/K) \cong G$ . We deal only with the case where  $G$  is of prime order  $\ell$ , and the base field  $K$  contains the  $\ell$ -th roots of unity. We can then describe these classes in terms of a "Stickelberger ideal" in the group ring  $\mathbb{Z}\Delta$  of the automorphism group  $\Delta$  of  $G$ .

### §1. The Main Theorem

(1.1) Let  $K$  be an algebraic number field with ring of integers  $O$ . If  $A$  is an  $O$ -order in a finite-dimensional semi-simple  $K$ -algebra, we write  $\text{Cl}(A)$  for the class group of  $A$ , the abelian group of stable isomorphism classes  $\text{cl}(M)$  of locally free rank one left  $A$ -modules  $M$ .

The class group is a functor of  $O$ -orders; if  $f: A \rightarrow B$  is a homomorphism of  $O$ -orders,  $f$  induces

$$\text{Cl}(f): \text{Cl}(A) \rightarrow \text{Cl}(B) \text{ by}$$

$$\text{cl}(M) \mapsto \text{cl}(f_* M), \text{ where:}$$

$$f_* M = B \otimes_A M.$$

(1.2) Let  $L/K$  be a finite Galois extension with  $G = \text{Gal}(L/K)$ . The ring  $\mathcal{O}_L$  of integers of  $L$  is an  $\mathcal{O}G$ -module, and one knows it is locally free (necessarily of rank 1) if and only if  $L/K$  is tame; that is,  $L/K$  is at most tamely ramified.

If we fix a finite group  $G$ , and let  $(L/K, h)$  range over the set of tame Galois extensions, with  $h: \text{Gal}(L/K) \xrightarrow{\sim} G$ , then  $\text{cl}(h_* \mathcal{O}_L)$  ranges over a set  $R(\mathcal{O}G) \subseteq \text{Cl}(\mathcal{O}G)$ . We call the elements of  $R(\mathcal{O}G)$  the realisable classes in  $\text{Cl}(\mathcal{O}G)$ .

Let  $\chi_0$  be the trivial character of  $G$ :  $\chi_0(\sigma) = 1$  for all  $\sigma \in G$ . Then  $\text{Cl}(\chi_0): \text{Cl}(\mathcal{O}G) \rightarrow \text{Cl}(\mathcal{O})$ , and we write:

$$\text{Cl}^0(\mathcal{O}G) = \text{Ker}(\text{Cl}(\chi_0)).$$

(1.2.1) Proposition: For any finite group  $G$  and any number field  $K$ :

$$R(\mathcal{O}G) \subseteq \text{Cl}^0(\mathcal{O}G).$$

We will prove this proposition in §2 below.

(1.3) Let  $\ell$  be a prime number. Assume from now on, except where the contrary is explicitly demanded, that  $G$  is of order  $\ell$  and that  $K$  contains the group  $\mu_\ell$  of  $\ell$ -th roots of unity.

Let  $\Delta = \text{Aut}(G)$ , the automorphism group of  $G$ ; we

write the action of  $\Delta$  exponentially, with the convention  $(a^\gamma)^\delta = a^{\delta\gamma}$ . For  $\delta \in \Delta$ , let  $t(\delta)$  be the unique integer such that:

$$(a) \quad 0 < t(\delta) < \ell, \text{ and}$$

$$(b) \quad \sigma^\delta = \sigma^{t(\delta)} \text{ for all } \alpha \in G.$$

Define:  $\theta = \sum_{\delta \in \Delta} t(\delta) \delta^{-1} \in \mathbb{Z} \Delta,$

and let:  $J = (\ell^{-1} \theta \cdot \mathbb{Z} \Delta) \cap \mathbb{Z} \Delta.$

Then  $J$  is an ideal of  $\mathbb{Z} \Delta$ .

By functoriality,  $\Delta$  acts on  $\text{Cl}(\mathcal{O}G)$ ; specifically:

$$\text{cl}(M)^\delta = \text{cl}(\delta_* M).$$

With this action,  $\text{Cl}^0(\mathcal{O}G)$  is a  $\Delta$ -submodule of  $\text{Cl}(\mathcal{O}G)$ .

(1.3.1) Theorem: Let  $G$  and  $K$  be as above. Then:

$$R(\mathcal{O}G) = \text{Cl}^0(\mathcal{O}G)^J,$$

the subgroup of  $\text{Cl}^0(\mathcal{O}G)$  generated by all  $c^\alpha$ ,  $c \in \text{Cl}^0(\mathcal{O}G)$ ,  $\alpha \in J$ . Moreover, given  $c' \in \text{Cl}^0(\mathcal{O}G)^J$ , and an ideal  $a$  of  $\mathcal{O}$ , there exists a tame Galois extension  $L/K$ , with discriminant prime to  $a$ , and  $h: \text{Gal}(L/K) \xrightarrow{\sim} G$  such that  $\text{cl}(h_* \theta_L) = c'$ .

The proof will be given in §4.

(1.3.2) Remark: (1.3.1) may be regarded as an analogue of the Stickelberger relations on the ideal class group of a cyclotomic field. With  $G$  as above and  $\zeta$  a primitive  $\ell$ -th root of unity, any non-trivial homomorphism  $G \rightarrow \mu_\ell$  induces an isomorphism  $\text{Cl}(\mathbb{Z}G) \cong \text{Cl}(\mathbb{Z}[\zeta])$ , ([18]). Since  $\text{Cl}(\mathbb{Z}) = 1$ ,  $\text{Cl}^0(\mathbb{Z}G) = \text{Cl}(\mathbb{Z}G)$ . We may identify  $\Delta$  with  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  by specifying the action  $\zeta^\delta = \zeta^{t(\delta)}$ . Then the isomorphism between  $\text{Cl}(\mathbb{Z}G)$  and  $\text{Cl}(\mathbb{Z}[\zeta])$  is a  $\Delta$ -isomorphism. The classical Stickelberger theorem ([20, p.355] or [2]) asserts in this case that  $\text{Cl}(\mathbb{Z}[\zeta])^J = 1$ . In fact, Hilbert's proof ([9, Satz 136]) shows that it is equivalent to the statement that every tame Galois extension of  $\mathbb{Q}$  of degree  $\ell$  has a "normal integral basis", i.e.  $R(\mathbb{Z}G) = 1$ . (\*) So:

$$R(\mathbb{Z}G) = \text{Cl}(\mathbb{Z}[\zeta])^J = \text{Cl}^0(\mathbb{Z}G)^J = 1.$$

## §2. Description of the Class Group

We now outline a procedure for finding  $\text{cl}(M)$ , when  $M$  is a rank 1 locally free  $\mathcal{O}G$ -module. Throughout, we use the notations of (1.3).

---

(\*) Footnote: The author is indebted to S.V. Ullom for this observation.



(2.1) Let  $X = \text{Hom}(G, \mu_\ell)$ , and let  $I$  be the group of fractional ideals of  $\mathcal{O}$  relatively prime to  $\ell$ . Then  $I^X$  is the group of functions  $X \rightarrow I$ . Let  $\mathcal{O}_\ell$  be the semilocalisation of  $\mathcal{O}$  at  $\ell$ :

$$\mathcal{O}_\ell = \{\alpha \in K \mid \alpha \text{ is integral at prime divisors of } \ell\}.$$

Let  $u(\mathcal{O}_\ell G)$  be the group of units of the ring  $\mathcal{O}_\ell G$ . We define a homomorphism  $f: u(\mathcal{O}_\ell G) \rightarrow I^X$  by:

$$\alpha \mapsto f_\alpha, \quad \text{where } f_\alpha(\chi) = \chi(\alpha) \cdot \alpha.$$

Then: (cf. [6]):

$$(2.1.1) \quad I^X / \text{Im}(f) \cong \text{Cl}(\mathcal{O}G).$$

(2.2) We now describe a homomorphism  $\phi: I^X \rightarrow \text{Cl}(\mathcal{O}G)$  which induces the isomorphism (2.1.1). Let  $M$  be a rank 1 locally free  $\mathcal{O}G$ -module. We may view  $M$  as embedded in  $V = K \otimes_{\mathcal{O}} M$ , and we have  $V \cong KG$  as  $KG$ -module. For each  $\chi \in X$ , let  $e_\chi$  be the idempotent of  $KG$  corresponding to  $\chi$ :

$$e_\chi = \ell^{-1} \sum_{\sigma \in G} \chi(\sigma) \sigma^{-1}.$$

Then:

$$(2.2.1) \quad \chi_* M \cong e_\chi \cdot M \quad (\subset V).$$

Indeed, (2.2.1) applies to any finite group  $G$  and any multiplicative  $\mathcal{O}$ -valued character  $\chi$  of  $G$ .

(2.2.2) Proof of (1.2.1): In the notation of (1.2.1), we have:

$$\chi_{0*}(\theta_L) \stackrel{\sim}{=} e_{\chi_0} \cdot \theta_L,$$

while if  $|G|$  is the order of  $G$ :

$$e_{\chi_0} \cdot \theta_L = |G|^{-1} \cdot \text{Tr}_{L/K}(\theta_L) = |G|^{-1} \cdot \theta,$$

since  $L/K$  is tame ([1,p.21]). So  $\text{cl}(\theta_L) \in \text{Cl}^0(\theta G)$ , as asserted.

Returning to the main argument, since  $M$  is locally free over  $\theta G$  and  $\theta_\ell$  is semilocal,  $\theta_\ell M$  is free over  $\theta_\ell G$ ,  $\theta_\ell M = \theta_\ell G \cdot v$ , say. The  $K$ -space  $e_\chi \cdot V = e_\chi^{KG} \cdot v$  is one-dimensional, so:

$$(2.2.3) \quad e_\chi^M = m(\chi) e_\chi^v,$$

for some  $m(\chi) \in I$ . Then  $m \in I^X$  and:

$$(2.2.4) \quad \phi(m) = \text{cl}(M).$$

(2.3) The group  $\Delta$  acts on  $X$  and  $I^X$  contravariantly:

$$\chi^\delta(\sigma) = \chi(\sigma^{\delta^{-1}}), \quad \chi \in X, \quad \delta \in \Delta, \quad \sigma \in G, \quad \text{and}$$

$$n^\delta(\chi) = n(\chi^{\delta^{-1}}), \quad n \in I^X.$$

It also acts on  $u(\theta_\ell G)$  and  $\text{Cl}(\theta G)$  (see 1.3). One verifies:

(2.3.1) The homomorphisms  $f: u(o_\ell G) \rightarrow I^X$  and  $\phi: I^X \rightarrow Cl(oG)$  are  $\Delta$ -homomorphisms.

Let  $X^\# = X - \{\chi_0\}$ . Then if  $n \in I^{X^\#}$  we may extend  $n$  to an element of  $I^X$  by setting  $n(\chi_0) = o$ . In this way, we may view  $I^{X^\#}$  as a  $\Delta$ -submodule of  $I^X$ .

(2.3.2) Proposition:  $\phi(I^{X^\#}) = Cl^0(oG)$ .

Further, if  $cl(M) \in Cl^0(oG)$  and  $cl(M) = \phi(m)$ , for some  $m \in I^X$ , then  $cl(M) = \phi(\tilde{m})$  where  $\tilde{m} \in I^{X^\#}$  is defined by:

$$\tilde{m}(\chi) = m(\chi) \cdot m(\chi_0)^{-1}.$$

Proof: By (2.2.1) and (2.2.3),  $cl(M) = \phi(m)$  lies in  $Cl^0(oG)$  if and only if  $m(\chi_0)$  is a principal ideal, so we have  $\phi(I^{X^\#}) \subseteq Cl^0(oG)$ .

If  $m(\chi_0)$  is principal,  $m(\chi_0) = a \cdot o$  say, then  $a$  is a unit of  $o_\ell$ , and hence also a unit of  $o_\ell G$ . The constant function  $\chi \mapsto m(\chi_0)$  is just  $f_a$  so that, in the notation of the statement, we have  $\phi(m) = \phi(\tilde{m})$  and  $cl(M) \in \phi(I^{X^\#})$ .

(2.4) Now choose a primitive  $\ell$ -th root of unity  $\zeta \in \mu_\ell$ , and put  $\lambda = (1 - \zeta)$ . Then  $\ell o = (\lambda)^{\ell-1}$ . If  $n$  is a non-

negative integer, we write  $R(\lambda^n)$  for the ray mod  $(\lambda^n)$ ; that is, the group of principal fractional ideals  $(a) \in I$  such that  $a \equiv 1 \pmod{(\lambda^n)^*}$ .

(2.4.1) Proposition:  $\phi(R(\ell)^X) = \phi(R(\ell)^{X\#}) = 1$ .

Proof: It is clearly enough to prove  $\phi(m) = 1$  for  $\phi \in R(\ell)^X$ .

For each  $\chi \in X$ , let  $m(\chi) = (m(\chi))$ , with

$m(\chi) \equiv 1 \pmod{(\ell)^*}$ , and define:

$$\beta = \sum_{\chi \in X} m(\chi) e_{\chi} \in KG.$$

Then  $1 - \beta \in \mathcal{O}_{\ell}G$ , and so  $\beta \in \mathcal{O}_{\ell}G$ . Similarly,

$\beta^{-1} = \sum_{\chi} m(\chi)^{-1} e_{\chi} \in \mathcal{O}_{\ell}G$ , and hence  $\beta \in u(\mathcal{O}_{\ell}G)$ . Then

$m = f_{\beta}$ , and we have  $\phi(m) = 1$ .

### §3. Calculation of $cl(\mathcal{O}_L)$

(3.1) Let  $L/K$  be a Galois extension of degree  $\ell$ ; then

$L/K$  is a Kummer extension,  $L = K(\omega)$  with  $\omega^{\ell} = w \in K^*$ , say. We

identify  $G$  with  $\text{Gal}(L/K)$  by choosing some  $\chi_1 \in X^{\#}$  and

specifying the  $G$ -action:

$$\sigma.\omega = \chi_1(\sigma)\omega, \quad \text{for all } \sigma \in G.$$

(3.1.1) Proposition (cf. [8, §39]): The extension  $L/K$  is

tame if and only if there is some  $b \in K^*$  such that:  
 $b_w^\ell \equiv 1 \pmod{(\lambda^\ell)^*}$ .

(3.1.2) Lemma: Let  $\ell$  be a prime divisor of  $\ell$  in  $L$ , and let  $\beta \in L^*$  be such that  $v_\ell(\beta) \geq 0$ . Then the following are equivalent:

$$(a) \quad v_\ell(\beta - 1) < v_\ell(\lambda);$$

$$(b) \quad v_\ell(\beta^\ell - 1) < v_\ell(\lambda^\ell);$$

$$(c) \quad v_\ell\left(\sum_{i=0}^{\ell-1} \beta^i\right) < v_\ell(\lambda^{\ell-1}).$$

Proof of (3.1.2): We have  $\beta^\ell - 1 = \prod_{i=0}^{\ell-1} (\beta - \zeta^i) = (\beta - 1) \cdot \sum_{i=0}^{\ell-1} \beta^i$ , so each of (a), (b), (c) implies that  $v_\ell(\beta - \zeta^i) < v_\ell(\lambda)$  for some  $i$ . This in turn implies  $v_\ell(\beta - \zeta^i) = v_\ell(\beta - \zeta^j)$  for all  $i$  and  $j$ . The lemma now follows.

(3.1.3) Remark: We have  $w \equiv 1 \pmod{(\lambda)^\ell}$  if and only if  $v_\ell(w^\ell - 1) \geq v_\ell(\lambda^\ell)$  for all prime divisors  $\ell$  of  $\ell$  in  $L$ . The lemma therefore shows  $w \equiv 1 \pmod{(\lambda)^\ell}$  if and only if:

$$\ell^{-1} \cdot \sum_{i=0}^{\ell-1} \omega^i \in o_\ell o_L.$$

Proof of (3.1.1): Since the degree  $[L:K]$  is  $\ell$ ,  $L/K$  is tame if and only if  $\text{Tr}_{L/K}(\sigma_\ell \theta_L) = \sigma_\ell$ .

Suppose first that  $L/K$  is tame; without loss of generality, we may assume that  $w \in u(\sigma_\ell)$ . Let  $v$  be an  $\sigma_\ell G$ -basis of  $\sigma_\ell \theta_L$ , so that:

$$\omega = \sum_{\sigma \in G} a_\sigma \cdot \sigma v,$$

for some  $a_\sigma \in \sigma_\ell$ . For any  $\tau \in G$ ,  $\tau\omega = \chi_1(\tau)\omega \equiv \omega \pmod{(\lambda)}$ , so that  $a_{\sigma\tau^{-1}} \equiv a_\sigma \pmod{(\lambda)}$ . Hence:

$$\omega \equiv a_1 \text{Tr}_{L/K}(v) \pmod{(\lambda)}.$$

Let  $b = a_1 \cdot \text{Tr}_{L/K}(v)$ . Then  $b^{-1}\omega \equiv 1 \pmod{(\lambda)^*}$ , and so:

$$b^{-\ell} \omega \equiv 1 \pmod{(\lambda)^{\ell}},$$

by (3.1.2).

For the converse, we may take  $w \equiv 1 \pmod{(\lambda)^{\ell}}^*$ . Let:

$$v = \ell^{-1} \cdot \sum_{i=0}^{\ell-1} \omega^i.$$

Then  $\text{Tr}_{L/K}(v) = 1$ . By (3.1.3),  $v \in \sigma_\ell \theta_L$ , so

$\text{Tr}_{L/K}(\sigma_\ell \theta_L) = \sigma_\ell$ , and  $L/K$  is tame.

(3.2) From now on, assume that  $L/K$  is tame and  $w \equiv 1 \pmod{(\lambda)^{\ell}}^*$ . The condition on  $w$  involves no loss of generality. We define a function  $\omega$  on  $X^\#$  by:

(3.2.1)  $w(\chi_1^n) = w^n$ , for  $0 < n < \ell$ ; that is:

$$w(\chi_1^{\delta^{-1}}) = w^{t(\delta)}.$$

(3.2.2) Theorem: For each  $\chi \in X^\#$ , let  $m(\chi)$  be the unique fractional ideal of  $\mathcal{O}$  such that  $m(\chi)^\ell \cdot (w(\chi))$  is integral and  $\ell$ -power free. Then  $m \in I^{X^\#}$  and:

$$\text{cl}(\mathcal{O}_L) = \phi(m).$$

Proof: Let 
$$v = \ell^{-1} \cdot \sum_{i=0}^{\ell-1} \omega^i.$$

By (3.1.3),  $v \in \mathcal{O}_\ell \mathcal{O}_L$ , and we claim  $\mathcal{O}_\ell \mathcal{O}_L = \mathcal{O}_\ell G.v$ . Let  $\sigma$  be some generator of  $G$ . Then  $\{\sigma^i v \mid 0 \leq i \leq \ell - 1\}$  and  $\{\omega^i \mid 0 \leq i \leq \ell - 1\}$  are  $K$ -bases of  $L$ , and we write  $d(\sigma^i v)$  and  $d(\omega^i)$  respectively for their discriminants. One finds:

$$d(\sigma^i v) = \ell^{-\ell} d(\omega^i) = \pm w^{\ell-1}.$$

So  $d(\sigma^i v)$  is, in particular, prime to  $\ell$ , and therefore  $v$  is an  $\mathcal{O}_\ell G$ -basis of  $\mathcal{O}_\ell \mathcal{O}_L$ , as asserted.

Now let  $n \in I^{X^\#}$  be given by:

$$e_\chi \cdot \mathcal{O}_L = n(\chi) \cdot e_\chi v.$$

By (2.2.4) and (2.3.2), it is enough to prove:



$$n(\chi_0) = \sigma, \quad \text{and } n(\chi) = m(\chi) \text{ for all } \chi \in X^\#.$$

Let  $\sigma' = \sigma[1/\ell]$ ,  $\theta'_L = \sigma' \cdot \theta_L$ . Then  $a \mapsto a' = a \cdot \sigma'$  induces an isomorphism between  $I$  and the group of fractional ideals of  $\sigma'$ . So, we are reduced to proving:

$$n'(\chi_0) = \sigma', \quad \text{and } n'(\chi) = m'(\chi) \text{ for all } \chi \in X^\#.$$

Since each  $e_\chi \in \sigma'G$ :

$$\begin{aligned} \theta'_L &= \bigoplus_{\chi} e_\chi \cdot \theta'_L \quad \text{and} \\ e_\chi \theta'_L &= \theta'_L \cap e_\chi K.G.v \end{aligned}$$

for all  $\chi$ . If  $\chi = \chi_1^i$ ,  $0 \leq i \leq \ell - 1$ ,  $e_\chi.v = \ell^{-1} \cdot \omega^i$ , so:

$$e_\chi \theta'_L = \theta'_L \cap K \cdot \omega^i = n'(\chi) \cdot \omega^i.$$

In particular, for  $i = 0$ ,  $\chi = \chi_0$ , and  $e_{\chi_0} \cdot \theta'_L = \theta'_L \cap K = \sigma'$ .

Hence  $n'(\chi_0) = \sigma'$ .

If  $0 < i < \ell$ , the condition  $n'(\chi) \cdot \omega^i = \theta'_L \cap K \cdot \omega^i$  implies that the  $\sigma'$ -ideal  $n'(\chi)^\ell \cdot (\omega^i)$  is integral and  $\ell$ -power free. For, if  $b'^\ell | n'(\chi)^\ell \cdot \omega^i$ , then  $b'^{-1} n'(\chi) \omega^i \subseteq \theta'_L \cap K \cdot \omega^i$ , which implies  $b' = \sigma'$ . So, by the definition of  $m$ ,

$$m'(\chi) = n'(\chi) \quad \text{for all } \chi \in X^\#,$$

and this completes the proof.

§4. The Stickelberger Condition

This section is devoted to the proof of the main theorem, (1.3.1).

(4.1) We continue to use the notations established in §3.

(4.1.1) Proposition: For each  $\delta \in \Delta$ ,  $\chi \in X^\#$ , there is an element  $b_\delta(\chi) \in K$ , which is a power of  $w$ , such that:

$$w^{\delta-t(\delta)}(\chi) = b_\delta^\ell(\chi).$$

Proof: Let  $\chi \in X^\#$ . Then  $\chi = \chi_1^{\gamma-1}$ , for some  $\gamma \in \Delta$ . So:

$$w^{\delta-t(\delta)}(\chi) = w(\chi^{\delta^{-1}}) \cdot w^{-t(\delta)}(\chi) = w^{t(\gamma\delta)-t(\gamma)t(\delta)}.$$

But  $t(\gamma\delta) \equiv t(\gamma) \cdot t(\delta) \pmod{\ell}$ , so the assertion follows.

(4.1.2) Proposition: There is a unique function  $a \in I^{X^\#}$  such that:

(i)  $a(\chi)$  is integral for all  $\chi \in X^\#$  ;

(ii)  $w(\chi) \cdot m^\ell(\chi) = a^\theta(\chi)$  for all  $\chi \in X^\#$  .

( $\theta$  is the Stickelberger element defined in (1.3)). Further, this function  $a$  satisfies:

(iii)  $b_\delta(\chi) \cdot m^{\delta-t(\delta)}(\chi) = a^{\ell^{-1}\theta \cdot (\delta-t(\delta))}(\chi)$  for all

$\delta \in \Delta$  and all  $\chi \in X^\#$  , and

(iv) the values  $a(\chi)$ ,  $\chi \in X^\#$  are square-free and relatively prime in pairs.

(The author is indebted to A. Fröhlich for this formulation of the Stickelberger relations.)

Proof: We assume first that a function  $a$  satisfying (i) and (ii) exists, and prove that it satisfies (iv). By the definition of  $m$  (in (3.2.2)),  $a^\theta(\chi)$  is  $\ell$ -power free for all  $\chi \in X^\#$ . But:

$$(4.1.3) \quad a^\theta(\chi) = \prod_{\delta \in \Delta} a^{t(\delta)\delta^{-1}}(\chi) = \prod_{\delta \in \Delta} a(\chi^\delta)^{t(\delta)}.$$

Let  $\tau \in \Delta$  be such that  $t(\tau) = \ell - 1$ . Then  $a(\chi^\tau)$  must be square-free, and prime to all other  $a(\chi^\delta)$ . As  $\chi$  runs over  $X^\#$ , so does  $\chi^\tau$ , which proves (iv).

Also, comparing (4.1.3) with (ii), we see that a prime  $p$  of  $K$  divides  $a(\chi)$  if and only if  $v_p(w(\chi)) \equiv 1 \pmod{\ell}$ , and further that  $a(\chi)$  is the product of all such  $p$ . This proves the uniqueness of the function  $a$ .

So, we define  $a(\chi)$  to be the product of all primes  $p$  of  $K$  such that  $v_p(w(\chi)) \equiv 1 \pmod{\ell}$ , and show that it satisfies (ii). (It clearly satisfies (i).) (4.1.1) shows that if  $\delta \in \Delta$ , and  $p$  is any prime of  $K$ , then:

$$v_p(w^{\delta^{-1}-t(\delta^{-1})}(\chi)) \equiv 0 \pmod{\ell}, \text{ so that}$$

$$v_p(w(\chi^\delta)) \equiv t(\delta^{-1})v_p(w(\chi)) \pmod{\ell}.$$

Hence,  $p$  divides  $a(\chi^\delta)$  if and only if  $v_p(w(\chi)) \equiv t(\delta) \pmod{\ell}$ .

So, by the definition of  $m$ :

$$w(\chi).m^\ell(\chi) = \prod_{\delta \in \Delta} a(\chi^\delta)^{t(\delta)} = a^\theta(\chi),$$

and (ii) is proved.

From (ii), we have:

$$w^{\delta-t(\delta)}(\chi).m^{\ell(\delta-t(\delta))}(\chi) = a^{\theta(\delta-t(\delta))}(\chi)$$

One knows (by (4.1.3) below) that  $\ell^{-1}\theta.(\delta - t(\delta)) \in \mathbb{Z}\Delta$ , so, by (4.1.1):

$$(b_\delta(\chi).m^{\delta-t(\delta)}(\chi))^\ell = (a^{\ell^{-1}\theta(\delta-t(\delta))}(\chi))^\ell.$$

The group  $I^{X\#}$  is torsion free, so (iii) follows.

Define

$$A = \{\alpha \in \mathbb{Z}\Delta \mid \ell^{-1}\theta.\alpha \in \mathbb{Z}\Delta\}.$$

(4.1.3)  $\ell^{-1}\theta.A = J$ , and  $A$  has a  $\mathbb{Z}$ -basis consisting of  $\ell$  and the elements  $\delta - t(\delta)$ , for  $\delta \neq 1$ .

Direct proof of this presents no difficulty; or see [10], [7].

(4.1.4) Proposition:  $\text{cl}(\theta_L) \in \text{Cl}^0(\mathcal{O}_G)^J$ .

Proof: By (3.2.2),  $\phi(m) = \text{cl}(\theta_L)$ . The functions  $x \mapsto (w(x))$ ,  $x \mapsto (b_\delta(x))$ , for fixed  $\delta$ , lie in the kernel of  $\phi$ , by (2.4.1). So we have:

$$\phi(m)^\ell = \phi(a)^\theta, \quad \text{and}$$

$$\phi(m)^{\delta-t(\delta)} = \phi(a)^{\ell^{-1}\theta(\delta-t(\delta))}$$

by (4.1.2). Thus (4.1.3) shows that  $\phi(m)^\alpha = \phi(a)^{\alpha \cdot \ell^{-1}\theta}$ , for all  $\alpha \in A$ . The proposition now follows from:

(4.1.5) Lemma: Let  $C$  be a  $\mathbb{Z}^\Delta$ -module, and let  $m \in C$ .

The following are equivalent:

(i) there exists  $a \in C$  such that  $m^\alpha = a^{\alpha \cdot \ell^{-1}\theta}$

for all  $\alpha \in A$ ;

(ii)  $m^\alpha \in C^J$  for all  $\alpha \in A$ ;

(iii)  $m \in C^J$ .

In particular, if  $C^J = 1$ , and  $m^\alpha = 1$  for all  $\alpha \in A$ , then  $m = 1$ .

Proof: Suppose first that  $C^J = 1$ , and that  $m^\alpha = 1$  for all  $\alpha \in A$ . Then  $m^\ell = 1$ , and  $m^{\delta-t(\delta)} = 1$  for all  $\delta$ . Thus:

$$m^\theta = \prod_{\delta \in \Delta} m^{t(\delta)\delta^{-1}} = \prod_{\delta \in \Delta} m^{t(\delta)t(\delta^{-1})} = m^{-1},$$

since  $\sum_{\delta \in \Delta} t(\delta) \cdot t(\delta^{-1}) \equiv -1 \pmod{\ell}$ . Hence:

$$m = m^{-\theta} \in C^J = 1.$$

Now, (i) implies (ii) since  $\alpha \cdot \ell^{-1}\theta \in J$  for all  $\alpha \in A$ . By applying the first part of the proof to the image of  $m$  in  $C/C^J$ , one sees that (ii) implies (iii). To show that (iii) implies (i), we may take  $m$  to be of the form  $n^{\ell^{-1}\theta \cdot \beta}$ ,  $\beta \in A$ ,  $n \in C$ . If we put  $a = n^\beta$ , then for all  $\alpha \in A$ ,

$$m^\alpha = n^{\beta \ell^{-1}\theta \alpha} = a^{\ell^{-1}\theta \alpha}.$$

(4.2) We now show that  $Cl^0(\mathcal{O}G)^J$  consists entirely of classes of rings of integers of extensions of  $K$ :

(4.2.1) Theorem: Let  $m \in Cl^0(\mathcal{O}G)^J$ . Then there is a tame Galois extension  $L/K$ , with  $G$  acting as Galois group, such that  $cl(\mathcal{O}_L) = m$ . Further,  $L/K$  may be chosen to have discriminant relatively prime to any given ideal of  $\mathcal{O}$ .

Proof: Choose  $\tilde{m} \in (I^{X^\#})^J$  such that  $\phi(\tilde{m}) = m$ . By (4.1.5), there is an  $\tilde{a} \in I^{X^\#}$  such that:

$$\tilde{m}^\alpha = \tilde{a}^{\alpha\ell^{-1}\theta}, \quad \text{for all } \alpha \in A.$$

Every coset of  $R(\lambda^\ell)$  in  $I$  contains infinitely many prime ideals. So, for each  $\chi \in X^\#$ , we may choose  $a(\chi)$  to lie in the same coset of  $R(\lambda^\ell)$  in  $I$  as  $\tilde{a}(\chi)$  so that the  $a(\chi)$  are distinct prime ideals relatively prime to any given ideal of  $\mathcal{O}$ . Then  $a^\theta(\chi)$  is integral,  $\ell$ -power free, and different from  $\mathcal{O}$  for all  $\chi$ .

If  $b_1, b_2 \in I^{X^\#}$ , we write  $b_1 \sim b_2$  to indicate that  $b_1(\chi)$  and  $b_2(\chi)$  lie in the same coset of  $R(\lambda^\ell)$  for all  $\chi \in X^\#$ . If  $b_1 \sim b_2$ , then  $\phi(b_1) = \phi(b_2)$ , by (2.4.1).

In particular we have  $\tilde{a} \sim a$ . Since  $\tilde{m}^\ell = \tilde{a}^\theta \sim a^\theta$ , we have:

$$\tilde{m}(\chi_1)^{-\ell} \cdot a^\theta(\chi_1) = w \cdot \mathcal{O}$$

for some  $w \equiv 1 \pmod{(\lambda^\ell)^*}$ . Here,  $\chi_1$  is the element of  $X^\#$  fixed in (3.1). This  $w$  is not an  $\ell$ -th power in  $K^*$  since  $a^\theta(\chi_1)$  is  $\ell$ -power free and different from  $\mathcal{O}$  by construction. Let  $L = K(\omega)$ , where  $\omega^\ell = w$ , and let  $G$  act on  $L$  by:

$$\sigma \cdot \omega = \chi_1(\sigma) \cdot \omega, \quad \text{for all } \sigma \in G.$$

We will show that  $\text{cl}(\mathcal{O}_L) = m$ .

First observe that  $L/K$  is tame, by (3.1.1).

Associated to  $L$  and  $w$ , we have the functions  $\omega, m$ , as in



(3.2.1) and (3.2.2). It will be enough to show  $m \sim \tilde{m}$ .

Since  $w(\chi_1) = w$ , we evidently have  $\tilde{m}(\chi_1) = m(\chi_1)$ .

We claim that the function  $a$  constructed above satisfies (ii) of (4.1.2). In order to show  $w(\chi) \cdot m^\ell(\chi) = a^\theta(\chi)$ , it is sufficient to show that  $w(\chi) \cdot a^{-\theta}(\chi)$  is an  $\ell$ -th power for each  $\chi \in X^\#$ , for it then must be  $m^{-\ell}(\chi)$  since  $a^\theta(\chi)$  is integral and  $\ell$ -power free. Recalling (4.1.1), for any  $\delta \in \Delta$ ,

$$(w \cdot a^{-\theta})^{\delta-t(\delta)}(\chi) = (b_\delta(\chi) \cdot a^{-\ell^{-1}\theta(\delta-t(\delta))}(\chi))^\ell.$$

Evaluating at  $\chi_1$ , we obtain:

$$w(\chi_1^{\delta^{-1}}) \cdot a^{-\theta}(\chi_1^{\delta^{-1}}) \cdot [w(\chi_1) a^{-\theta}(\chi_1)]^{-t(\delta)} \in I^\ell.$$

But  $w(\chi_1) \cdot a^{-\theta}(\chi_1) = m^{-\ell}(\chi_1)$  so that:

$$w(\chi_1^{\delta^{-1}}) \cdot a^{-\theta}(\chi_1^{\delta^{-1}}) \in I^\ell,$$

and our claim is proved.

Now, by (4.1.2) (iii), for any  $\delta \in \Delta$ ,

$$m^{\delta-t(\delta)} \sim a^{\ell^{-1}\theta(\delta-t(\delta))} \sim \tilde{a}^{\ell^{-1}\theta(\delta-t(\delta))} = \tilde{m}^{\delta-t(\delta)}.$$

Evaluating at  $\chi_1$  we have:

$$m(\chi_1^{\delta^{-1}}) \cdot m(\chi_1)^{-t(\delta)} \sim \tilde{m}(\chi_1^{\delta^{-1}}) \cdot \tilde{m}(\chi_1)^{-t(\delta)}$$

We have already observed that  $m(\chi_1) = \tilde{m}(\chi_1)$ , so that  $m(\chi_1^{\delta^{-1}}) \sim \tilde{m}(\chi_1^{\delta^{-1}})$  for all  $\delta$ , and hence  $m \sim \tilde{m}$ ; so

$$m = \text{cl}\left(\frac{0}{L}\right).$$

Finally observe that any prime ramified in  $L/K$  must divide  $a^\theta(\chi_1)$ , so that proper choice of  $a$  guarantees that the discriminant of  $L/K$  is prime to any given ideal of  $\mathcal{O}$ .

## §5. Corollaries

(5.1) We now consider the problem of estimating the index  $(\text{Cl}^0(\mathcal{O}G):R(\mathcal{O}G))$ .

(5.1.1) Theorem: Let  $\ell = 2$ . Then  $R(\mathcal{O}G) = \text{Cl}^0(\mathcal{O}G)$ .

Proof: In this case,  $\Delta = 1$ ,  $\ell^{-1}\theta = 1/2$ , and  $J = \mathbb{Z}$ .

Let  $C(\ell) = I/R(\ell)$  be the ray class group mod  $\ell$ , and  $C = \text{Cl}(\mathcal{O})$  the ordinary ideal class group, of  $K$ .

(5.1.2) Theorem: There are  $\mathbb{Z} \Delta$ -epimorphisms:

$$C(\ell)^{X\#} / (C(\ell)^{X\#})^J \twoheadrightarrow \text{Cl}^0(\mathcal{O}G)/R(\mathcal{O}G), \text{ and}$$

$$\text{Cl}^0(\mathcal{O}G)/R(\mathcal{O}G) \twoheadrightarrow C^{X\#} / (C^{X\#})^J.$$

Proof: The inclusions (see (2.4.1))  $R(\ell)^{X\#} \subseteq \text{Ker}(\phi) \subseteq R(1)^{X\#}$

induce epimorphisms on the corresponding quotients of  $I^{X\#}$ :

$$C(\ell)^{X\#} \twoheadrightarrow Cl^0(\mathcal{O}_G) \twoheadrightarrow C^{X\#}.$$

The result now follows from (1.3.1).

Now assume that  $\ell$  is odd and let  $\tau$  be the unique element of  $\Delta$  of order 2. Define:

$$\mathbb{Z}\Delta^- = \{\alpha \in \mathbb{Z}\Delta \mid \tau\alpha = -\alpha\}, \text{ and } \mathcal{J}^- = \mathcal{J} \cap \mathbb{Z}\Delta^-.$$

Then one knows ([10]) that  $(\mathbb{Z}\Delta^- : \mathcal{J}^-) = h^-$ , the "first factor" of the class number of  $\mathbb{Q}(\zeta)$ , where  $\zeta$  is a primitive  $\ell$ -th root of unity. Further, it follows from [10] that:

$$(5.1.3) \quad \mathbb{Z}\Delta/\mathcal{J} \cong \mathbb{Z}^{((\ell-3)/2)} \oplus T,$$

where  $T$  is a finite abelian group of order  $h^-$ .

(5.1.4) Proposition: Let  $B$  be an abelian group. Then  $B^{X\#}/(B^{X\#})^{\mathcal{J}} \cong (\mathbb{Z}\Delta/\mathcal{J}) \otimes B$ .

Proof: The map  $B^{X\#} \rightarrow \mathbb{Z}\Delta \otimes B$  given by:

$$f \mapsto \sum_{\delta \in \Delta} \delta \otimes f(\chi_1^\delta)$$

is a  $\Delta$ -isomorphism. Also, in the exact sequence:

$$J \otimes B \rightarrow \mathbb{Z} \Delta \otimes B \rightarrow (\mathbb{Z} \Delta / J) \otimes B \rightarrow 0 ,$$

the image of  $J \otimes B$  in  $\mathbb{Z} \Delta \otimes B$  is clearly  $(\mathbb{Z} \Delta \otimes B)^J$ . The result follows.

(5.1.5) Remark:

The index  $(Cl^0(\mathcal{O}G):R(\mathcal{O}G))$  can now be estimated by applying (5.1.4) to the groups  $C(\ell)$  and  $C$ , using (5.1.2). More precisely, it follows from (5.1.3) that:

$$\mathbb{Z} \Delta / J \cong \bigoplus_{i=1}^{(\ell+1)/2} \mathbb{Z} / b_i \mathbb{Z} \oplus \mathbb{Z}^{((\ell-3)/2)}$$

for positive integers  $b_i$  such that  $b_i | b_{i+1}$  and

$b_1 b_2 \dots b_{(\ell+1)/2} = h^-$ . Then, if  $B$  is finite abelian:

$$B^{X\#} / (B^{X\#})^J \cong \bigoplus_{i=1}^{(\ell+1)/2} B / B^{b_i} \oplus B^{((\ell-3)/2)} .$$

Information about the structure of  $B$  and the  $b_i$  can then be used to estimate the order of the right hand side. In this regard, consider the following:

(5.1.6) Exercise: Show that  $b_i = 1$  for  $i \leq \langle \sqrt{4\ell+1} \rangle - 2$ ,

where  $\langle \alpha \rangle$  denotes the least integer  $\geq \alpha$ . (Hint: the matrix  $([ij/\ell])$  expresses a set of generators of  $J$  in terms of a basis of  $\mathbb{Z} \Delta$ .)

Now let  $D(\mathcal{O}G)$  denote the kernel of  $Cl^0(\mathcal{O}G) \rightarrow C^{X\#}$ ;  
cf. [6].

(5.1.7) Theorem:  $R(\mathcal{O}G) \subseteq D(\mathcal{O}G)$  if and only if  $K$  has class number  $h_K = 1$ .

Proof: By (5.1.6),  $b_1 = 1$ , so that if  $C \neq 1$ , we must have  $(C^{X\#} : (C^{X\#})^J) < |C^{X\#}|$ . Consequently,  $R(\mathcal{O}G) = Cl^0(\mathcal{O}G)^J$  has non-trivial image in  $C^{X\#}$ . The converse is clear.

(5.2) Forgetting the action of  $G$  induces a homomorphism

$$i^* : Cl(\mathcal{O}G) \rightarrow C.$$

We write  $r(\mathcal{O}, G)$  for the image  $i^* R(\mathcal{O}G)$ . In [14],  $r(\mathcal{O}, G)$  was determined in the more general situation where  $G$  is cyclic of order  $n$  and  $K$  contains the  $n$ -th roots of unity. In [12], [13], and [3], Long and Endo have determined  $r(\mathcal{O}, G)$  for a number of groups, including abelian groups of odd order and certain metacyclic groups, with no restriction on the base field  $K$ . Here we recover the result in [14] for the case when  $G$  is of prime order  $\ell$ .

(5.2.1) Proposition: If  $C$  is viewed as a  $\mathbb{Z}\Delta$ -module with

trivial  $\Delta$ -action, the homomorphism  $i^*$  is a  $\Delta$ -homomorphism. If  $n \in I^X$ , then  $i^* \phi(n)$  is the class of the ideal  $\prod_{\chi \in X} n(\chi)$ . In particular,  $i^* \text{Cl}^0(\mathcal{O}G) = C$ .

Proof: If  $M$  is a rank one locally free  $\mathcal{O}G$ -module,  $i^* \text{cl}(M)$  is the Steinitz class of  $M$  viewed as an  $\mathcal{O}$ -module. So  $i^* \text{cl}(M)$  is the ideal class of the module index  $(F:M)_{\mathcal{O}}$  (see [1, p.10]), where  $F$  is any free  $\mathcal{O}$ -module spanning  $K \otimes_{\mathcal{O}} M$ . As in (2.2), we may choose the module  $F$  to be a free  $\mathcal{O}G$ -module such that  $\mathcal{O}_{\ell} F = \mathcal{O}_{\ell} M$ . The module index  $(F:M)_{\mathcal{O}}$  may be identified with  $(\mathcal{O}'F:\mathcal{O}'M)_{\mathcal{O}'}$ , where  $\mathcal{O}' = \mathcal{O}[1/\ell]$ , since it is prime to  $\ell$ . As in the proof of (3.2.2), we obtain:

$$\mathcal{O}'M = \bigoplus_{\chi \in X} \mathcal{O}'n(\chi) \cdot e_{\chi} v, \quad \text{and} \quad \mathcal{O}'F = \bigoplus_{\chi \in X} \mathcal{O}' \cdot e_{\chi} v,$$

where  $F = \mathcal{O}G.v$ . So  $(\mathcal{O}'F:\mathcal{O}'M)_{\mathcal{O}'} = \prod_{\chi} \mathcal{O}'n(\chi)$ , and hence  $(F:M)_{\mathcal{O}} = \prod_{\chi} n(\chi)$ . The second assertion follows.

For any  $\delta \in \Delta$ ,  $\prod_{\chi} n(\chi) = \prod_{\chi} n(\chi^{\delta})$ , which proves the first assertion.

For a positive integer  $d$ , let  $C^d$  denote the group of  $d$ -th powers in  $C$ .

(5.2.2) Theorem: Let:

$$d(\ell) = \begin{cases} (\ell - 1)/2 & \text{if } \ell \text{ is odd;} \\ 1 & \text{if } \ell = 2. \end{cases}$$

Then  $r(o, G) = c^{d(\ell)}$ .

Proof: If  $\ell = 2$ , the result follows directly from (5.1.1) and (5.2.1). So assume  $\ell$  is odd, and let  $\epsilon : \mathbb{Z} \Delta \rightarrow \mathbb{Z}$  be the augmentation homomorphism. For any  $c \in C$ ,  $\alpha \in \mathbb{Z} \Delta$ , we have  $i^*(c^\alpha) = (i^*c)^{\epsilon(\alpha)}$ , by (5.2.1). Now,

$$\epsilon(\theta) = \sum_{\delta \in \Delta} t(\delta) = \ell(\ell - 1)/2, \text{ and so, for } \delta \in \Delta:$$

$$\epsilon((\delta - t(\delta)) \cdot \ell^{-1} \theta) = (1 - t(\delta)) \cdot (\ell - 1)/2.$$

Therefore  $\epsilon(J) = ((\ell - 1)/2) \cdot \mathbb{Z}$ , and:

$$r(o, G) = i^*(cl^0(oG)^J) = c^{(\ell-1)/2}.$$

#### REFERENCES

1. J.W.S. Cassels & A. Fröhlich, Algebraic Number Theory (Academic Press, London 1967).
2. J. Coates, p-adic L-functions and Iwasawa's theory, Durham Symposium.
3. L.P. Endo, Steinitz classes of tamely ramified Galois extensions of algebraic number fields (thesis, University of Illinois, 1975).



4. A. Fröhlich, The module structure of Kummer extensions over Dedekind domains, J. reine u. angew. Math., 209 (1962), 39-53.
5. A. Fröhlich, Locally free modules over arithmetic orders, J. reine u. angew. Math., 274/275 (1975) 112-124.
6. A. Fröhlich, Galois module structure, Durham Symposium.
7. A. Fröhlich, Stickelberger without Gauss sums, Durham Symposium.
8. E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, 2te Aufl. (Akademische Verlag, Leipzig, 1954).
9. D. Hilbert, Bericht: Die Theorie der algebraischen Zahlkörper, Jber. dt. MathVerein., 4(1897), 175-546.
10. K. Iwasawa, A class number formula for cyclotomic fields, Ann. Math., 76 (1962), 171-179.
11. H. Jacobinski, Genera and decomposition of lattices over orders, Acta Math., 121 (1968), 1-29.
12. R.L. Long, Steinitz classes of cyclic extensions of prime degree, J. reine u. angew. Math., 250 (1971), 87-98.
13. R.L. Long, Steinitz classes of cyclic extensions of degree  $\ell^r$ , Proc. A.M.S., 49 (1975) 297-304.
14. L.R. McCulloh, Cyclic extensions without integral bases, Proc. A.M.S., 17 (1966), 1191-1194.
15. J. Milnor, Introduction to algebraic K-theory, Ann. Math. Studies 72 (Princeton Univ. Press, 1972).
16. E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, J. reine u. angew. Math., 167 (1931), 147-152.

17. I. Reiner & S.V. Ullom, Class groups of integral group rings, Trans. A.M.S., 170 (1972), 1-30.
18. D.S. Rim, Modules over finite groups, Ann. Math., 69 (1959), 700-712.
19. J-P. Serre, Représentations linéaires des groupes finis, 2ième éd. (Hermann, Paris, 1971).
20. L. Stickelberger, Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann., 37 (1890), 321-367.

# Stickelberger without Gauss sums

A. Fröhlich

## §1. Introduction

The ideal class group of a cyclotomic field  $K$ , when viewed as a module over the absolute Galois group  $\Gamma$ , satisfies certain relations, first discovered by Stickelberger (cf. [1] (Theorem 3.1)), i.e. with  $\beta$  running through a certain subset  $S$  of the integral group ring  $\mathbb{Z}(\Gamma)$  (which may be taken as an ideal), and for all ideal classes  $C$  of  $K$ , one has

$$(1.1) \quad C^\beta = 1.$$

One proves this by showing that

$$(1.2) \quad p^\beta \text{ is principal in } K,$$

for all  $\beta \in S$  and almost all prime ideals  $p$ .

The main purpose of the present note is to give a new proof of (1.2) for prime ideals  $p$  of the first degree, and hence a new proof of (1.1), in the case of fields  $K$  of roots of unity. We shall first establish a more general,

but quite elementary Proposition and then deduce (1.2) as a special case, using as additional information in that special case the existence of a normal integral basis in tame cyclotomic fields ("Hilbert-Speiser theorem"), together with some other even more elementary facts about those fields. We shall also discuss briefly some other aspects and consequences of our basic proposition.

Our approach exhibits further evidence for the interconnection between three seemingly distinct aspects of algebraic number theory, namely Galois module structure of ideal class groups, Gauss sums, and Galois module structure of rings of algebraic integers. It is of interest to recall here some relevant previous work. Cougnard has applied the Stickelberger relations to obtain, for certain absolutely normal fields, results on the Galois module structure of algebraic integers, (cf. [2], [3]). On the other hand I have discovered a general theorem relating Galois Gauss sums and Galois module structure of algebraic integers for relatively normal and tame extensions (cf. [4]). For Abelian characters these Gauss sums are essentially just products of Gauss sums for finite fields. In the third place recall that the main ingredient in the

usual proof of Stickelbergers theorem on the ideal class group as Galois module is the prime decomposition law of Gauss sums for finite fields (also due to Stickelberger (cf. [1], (Prop. 3.8))). Finally in the new proof this is replaced by the Hilbert-Speiser theorem which deals with the Galois module structure of cyclotomic integers. In fact we shall here not only not make use of the prime decomposition law of Gauss sums, but shall recover this law, at least in the case when the relevant finite field is a prime field.

My approach had been stimulated by the work of L. McCulloh on Kummer extensions of prime degree, although there is little actual overlap (see [5]). I also owe to McCulloh a further simplification in my own proof.

## §2. Module theory

Throughout this section  $f$  is an integer  $> 1$ ,  $\Gamma$  is a finite group and  $c: \Gamma \rightarrow (\mathbb{Z}/f\mathbb{Z})^*$  a surjective homomorphism of  $\Gamma$  onto the group of units of the residue class ring  $\mathbb{Z}/f\mathbb{Z}$ . If  $1 < d|f$  we write  $c_d: \Gamma \rightarrow (\mathbb{Z}/d\mathbb{Z})^*$  for the compositum of  $c$  and the canonical quotient map  $(\mathbb{Z}/f\mathbb{Z})^* \rightarrow (\mathbb{Z}/d\mathbb{Z})^*$ . If  $\gamma \in \Gamma$  we shall write  $t_d(\gamma)$  for the integer with  $c_d(\gamma) = t_d(\gamma) \bmod d$  and  $0 \leq t_d(\gamma) < d$ . We

may and shall also view  $c_d$  and  $t_d$  as functions on the quotient group  $\Gamma/\text{Ker } c_d$ . Finally we set

$$\theta_d = \frac{1}{d} \sum_{\gamma \in \Gamma/\text{Ker } c_d} \gamma t_d(\gamma).$$

Thus  $\theta_d$  lies in the rational group ring  $\mathbb{Q}(\Gamma/\text{Ker } c_d)$  and  $d \theta_d$ , and a fortiori  $f \theta_d$  lie in  $\mathbb{Z}(\Gamma/\text{Ker } c_d)$ .

Lemma 1. Let  $M$  be a  $\Gamma$ -module. Then  $(M^{\text{Ker } c_d}$  is a  $\Gamma/\text{Ker } c_d$ -module and) for  $v \in M^{\text{Ker } c_d}$

$$v(f \theta_d)(\gamma t_f(\gamma) - 1) \in f M, \quad \text{for all } \gamma \in \Gamma.$$

Next let  $X$  be a  $\Gamma$ -set, not necessarily finite and  $F(X)$  the free  $\mathbb{Z}$ -module on  $X$  made into a  $\Gamma$ -module via the action of  $\Gamma$  on  $X$ . If  $r > 1$  we say  $v \in F(X)$  is  $r$ -power free ("square free" if  $r = 2$ ), if in the expansion

$$v = \sum_{x \in X} a_x x, \quad a_x = a_x(v) \in \mathbb{Z}$$

we have

$$0 \leq a_x < r.$$

We say  $v$  and  $w$  are coprime if, for all  $x$ ,  $a_x(v) = 0$  or  $a_x(w) = 0$ .

Lemma 2. Let  $v \in F(X)$ , so that for all  $\gamma \in \Gamma$ ,

$$v(t_f(\gamma)\gamma - 1) \in fF(X).$$

Then

$$(i) \quad v \equiv \sum_{1 < d | f} v(d) (f \ominus_d) \pmod{fF(X)},$$

or if  $v$  is  $f$ -power free actually

$$(ii) \quad v = \sum_{1 < d | f} v(d) (f \ominus_d),$$

where

(iii) for each  $d$ ,  $v(d) \in F(X)$  is square free and fixed under  $\text{Ker } c_d$ ,

(iv) for  $d \neq e \mid f$ , and for all  $\gamma$ ,  $v(d)$  and  $v(e)\gamma$  are coprime.

(v) for each  $d$  and for  $\gamma, \delta \in \Gamma/\text{Ker } c_d$ ,  $\gamma \neq \delta$  also  $v(d)\gamma$  and  $v(d)\delta$  are coprime.

These conditions determine the  $v(d)$  uniquely.

If moreover  $\Gamma$  acts freely on  $X$ , then for some  $v'$

$$(vi) \quad v \equiv v' \sum_{\gamma \in \Gamma} \gamma t_f(\gamma).$$

In the next Lemma we shall view  $\mathbb{Q}(\Gamma/\text{Ker } c_d)$  as a  $\mathbb{Q}(\Gamma)$ -module, via  $\Gamma \rightarrow \Gamma/\text{Ker } c_d$ .

Lemma 3. The following conditions on an element  $\rho$  of  $\mathbb{Z}(\Gamma)$  are equivalent.



- (i)  $\rho$  lies in the  $\mathbb{Z}$ -module  $(\mathbb{Z}(\Gamma)\text{-ideal}) \ E$  generated by  $f\mathbb{Z}(\Gamma)$  and the elements  $\gamma t_f(\gamma) - 1$  for all  $\gamma$ ,
- (ii)  $\rho \theta_f \in \mathbb{Z}(\Gamma/\text{Ker } c)$ ,
- (iii)  $\rho \theta_d \in \mathbb{Z}(\Gamma/\text{Ker } c_d)$ , for all  $d$ .

Proof of Lemma 1. We go over to  $M/fM$ , i.e., we consider a module  $N$  over  $(\mathbb{Z}/f\mathbb{Z})(\Gamma)$ . We can then define a new action  $y, \gamma \mapsto y \cdot \gamma$  of  $\Gamma$  on  $N$  by  $y \cdot \gamma = \gamma c(\gamma) \gamma$ . If now  $y\delta = y$  for all  $\delta \in \text{Ker } c_d$  then also  $(\frac{f}{d})y \cdot \delta = (\frac{f}{d})y$ , and moreover  $(\frac{f}{d})y \cdot \sum_{\gamma \in \Gamma/\text{Ker } c_d} \gamma$  is fixed under  $\Gamma$ , for the new action. This is exactly the assertion of the Lemma.

With  $X$  as in Lemma 2, next let  $N$  be the free  $\mathbb{Z}/f\mathbb{Z}$ -module on  $X$  made into a  $(\mathbb{Z}/f\mathbb{Z})(\Gamma)$ -module via the action of  $\Gamma$  on  $X$ . A square free element  $y$  of  $N$  is one for which in the expansion  $y = \sum_{x \in X} a_x x$  ( $a_x \in \mathbb{Z}/f\mathbb{Z}$ ) we have  $a_x = 0$  or  $a_x = 1$ . We can again speak of two elements being coprime, just as for the module  $F(X)$ . We shall establish

Lemma 4. Let  $y \in N$ , with  $y(\gamma c(\gamma) - 1) = 0$  for all  $\gamma \in \Gamma$ .

Then

$$(i) \quad y = \sum_{1 < d | f} [(y(d) \frac{f}{d}) \sum_{\gamma \in \Gamma/\text{Ker } c_d} c_d(\gamma) \gamma]$$

where

(ii) for each  $d$ ,  $y(d) \in N$  is fixed under  $\text{Ker } c_d$  and square free,

(iii) for  $d \neq e \mid f$ , and for all  $\gamma$ ,  $y(d)$  and  $y(e)\gamma$  are coprime,

(iv) for each  $d$  and for  $\gamma, \delta \in \Gamma / \text{Ker } c_d$ ,  $\gamma \neq \delta$ , also  $y(d)\gamma$  and  $y(d)\delta$  are coprime.

Properties (i)-(iv) determine the  $y(d)$  uniquely.

Proof of Lemma 4. Every element  $y$  of  $N$  has a unique representation

$$(2.1) \quad y = \sum_{b \in \mathbb{Z} / f\mathbb{Z}} by_b$$

where the  $y_b$  are square free and mutually orthogonal.

Clearly

$$(2.2) \quad \begin{cases} y_b \gamma = (y\gamma)_b & \text{for } \gamma \in \Gamma \\ (yc)_b = y_{c^{-1}b} & \text{for } c \in (\mathbb{Z} / f\mathbb{Z})^* \end{cases}$$

Now suppose that  $yc(\gamma)\gamma = y$  for all  $\gamma \in \Gamma$ . By (2.2)

$$(2.3) \quad y_b \gamma = y_{c(\gamma)b} \quad .$$

Let  $1 < d \mid f$  and let  $I_d$  be the set of elements  $b$  of  $\mathbb{Z} / f\mathbb{Z}$

which generate the same ideal (b) as (the class of)  $f/d$ . If  $b \in I_d$  then, by (2.3),  $y_b^\delta = y_b$  for all  $\delta \in \text{Ker } c_d$  and thus  $y_b \gamma$  is well defined for  $\gamma \in \Gamma/\text{Ker } c_d$ . Now the action of  $(\mathbb{Z}/f\mathbb{Z})^*$  on  $I_d$  defines an action of  $(\mathbb{Z}/d\mathbb{Z})^*$ . Every element of  $I_d$  is then uniquely of the form  $(f/d) c_d(\gamma)$ ,  $\gamma \in \Gamma/\text{Ker } c_d$ . Thus by (2.3)

$$\sum_{b \in I_d} b y_b = y_{f/d} \left( \frac{f}{d} \right) \sum_{\gamma \in \Gamma/\text{Ker } c_d} \gamma c_d(\gamma),$$

(Here we have used the same symbol for  $f/d$  and for its class mod  $f$ .) This then yields (i) and (ii) with  $y(d) = y_{f/d}$ . (iii) and (iv) follow from the fact that the  $y_b$  are mutually coprime. Conversely by the uniqueness of (2.1) we see that if conditions (i) - (iv) hold then  $y(d) = y_{f/d}$ .

Proof of Lemma 2. Let  $\pi: F(X) \rightarrow N = F(X)/fF(X)$  be the "residue class map" mod  $f$ . On the set  $F(X)^\wedge$  of  $f$ -power free elements  $\pi$  is a bijection. Let  $\upsilon: N \rightarrow F(X)^\wedge$  be the inverse bijection. Then both  $\pi$  and  $\upsilon$  preserve  $\Gamma$ -action, square freeness and orthogonality. If now  $v$  satisfies the hypothesis of Lemma 2, then  $\pi(v) = y$  satisfies the hypothesis of Lemma 4, hence satisfies conditions (i) - (iv) of Lemma 4. It follows now that  $\upsilon\pi(v) = \sum_{1 \leq d/f} v(d) (f \circ_d)$ , with the  $v(d)$

satisfying (iii)-(v) in Lemma 2. On the other hand  $v \equiv v\pi(v)$  (mod  $fF(X)$ ) and if  $v \in F(X)'$  then  $v = v\pi(v)$ , i.e., we have (i), and (ii) respectively. Uniqueness follows from Lemma 4 via the inverse bijections  $v$  and  $\pi$ .

Now assume that  $\Gamma$  acts freely on  $X$ . As  $v(d)$  is fixed under  $\text{Ker } c_d$ ,

$$v(d) = \sum_{\delta \in \text{Ker } c_d} w\delta, \quad \text{some } w \in F(X).$$

For every  $\gamma \in \Gamma$ ,  $\delta \in \text{Ker } c_d$  we have  $(\frac{f}{d}) t_d(\gamma) \equiv (\frac{f}{d}) t_f(\delta\gamma)$  (mod  $f$ ). Hence

$$v(d) (f \theta_d) \equiv \sum_{\gamma \in \Gamma} (\frac{f}{d}) w\gamma t_f(\gamma).$$

This together with (i) implies (vi).

Proof of Lemma 3. (i)  $\rightarrow$  (iii): In fact if  $\rho$  satisfies the conditions of (i) then by Lemma 1,  $\rho f \theta_d \in f\mathbb{Z}(\Gamma/\text{Ker } c_d)$ , for all  $d$ , and this implies (iii).

(iii)  $\rightarrow$  (ii). Trivial.

(ii)  $\rightarrow$  (i). Let  $E$  be the  $\mathbb{Z}$ -module generated by  $f\mathbb{Z}(\Gamma)$  and the  $\gamma t_f(\gamma) - 1$ , and let  $E'$  be the  $\mathbb{Z}$ -module of elements  $\rho$  of  $\mathbb{Z}(\Gamma)$  satisfying (ii). Then  $\gamma - t_f(\gamma^{-1}) \in E$ . Thus if  $\rho = \sum a_\gamma \gamma \in E'$ , then  $\rho \equiv \sum a_\gamma t_f(\gamma^{-1})$  (mod  $E$ ). We already know that  $E \subset E'$ . Thus

$\sum a_{\gamma} t_f(\gamma^{-1}) \in E' \cap \mathbb{Z} = f\mathbb{Z} \subset E$ . Hence  $\rho \in E$ .

### §3. Kummer theory

Here  $K$  is an algebraic number field, of finite degree over  $\mathbb{Q}$  and containing the primitive  $f$ -th roots of unity. We shall write  $\mu_f$  for the group of  $f$ -th roots of unity in  $K$ .

The symbol  $\Omega_f$  stands for the Galois group  $\text{Gal}(K(K^{*1/f})/K)$ , where  $K(K^{*1/f})$  is the composite field of the extensions  $K(a^{1/f})$  with  $a \in K^*$  (the multiplicative group of  $K$ ).

Finally  $\Psi_f$  is the group of continuous homomorphisms

$\Omega_f \rightarrow \mu_f$ . If  $a \in K^*$ ,  $\omega \in \Omega_f$  define

$$\langle a, \omega \rangle = (a^{1/f})^{\omega-1}.$$

This yields a pairing

$$K^*/K^{*f} \times \Omega_f \rightarrow \mu_f,$$

which in turn gives rise to an isomorphism

$$(3.1) \quad K^*/K^{*f} \cong \Psi_f.$$

Let  $\psi \in \Psi_f$ . The elements  $x$  of  $K(K^{*1/f})$  with  $x^{\omega-1} = \psi(\omega)$  for all  $\omega \in \Omega_f$ , form a one dimensional  $K$ -space  $V(\psi)$  and the algebraic integers in  $V(\psi)$  form a finitely generated rank one module  $P(\psi)$  over the ring  $\mathcal{O}$  of algebraic integers in  $K$ .

Its Steinitz class will be denoted by  $\text{cl}(P(\psi))$ . These classes give information on integral Galois module structure. On the other hand we also consider the  $\mathcal{O}$ -module

$$P(\psi)^f = a(\psi)$$

generated by the products  $\prod_{i=1}^f x_i$  with  $x_i \in P(\psi)$ . This is actually an  $f$ -power free integral ideal of  $\mathcal{O}$  which gives information on ramification. Our principal result will imply a relation between these invariants.

Now let  $a$  be an element of  $K^*$  (whose class mod  $K^{*f}$  is) corresponding to  $\psi \in \Psi_f$  (cf. (3.1)). Then for  $\alpha^f = a$  we have

$$(3.2) \quad V(\psi) = \alpha K, \quad P(\psi) = \alpha b$$

for some fractional ideal  $b$  of  $\mathcal{O}$ . Clearly then

$$(3.3) \quad \text{cl}(P(\psi)) = \text{cl}(b),$$

while on taking  $f$ -th powers we get

$$(3.4) \quad (a) = a(\psi) b^{-f}.$$

Thus  $a(\psi)$  is the " $f$ -power free integral part" of  $(a)$ .

Keeping to the notation just introduced, we now recall in a special case some elementary aspects of resolvent theory. Let  $N$  be a normal extension of finite degree of  $K$  with Galois group  $\Delta = \text{Gal}(N/K)$ . Suppose  $\alpha \in N$ , hence  $V(\psi) \subset N$  (see (3.2)). We then may view  $\psi$  as character of

$\Delta$ , i.e., as an element of  $\text{Hom}(\Delta, \mu_f)$ . If  $x \in N$  we define the Lagrange resolvent by

$$(3.5) \quad (x|\psi) = \sum_{\delta \in \Delta} x^{\delta} \psi(\delta)^{-1}.$$

We shall say that  $x$  generates a normal integral basis of  $N/K$  if the conjugates  $x^{\delta}$  form an  $\mathcal{O}$ -basis of the ring of algebraic integers in  $N$ .

Lemma 5. Suppose  $x$  generates a normal integral basis of  $N/K$ . Then

$$(i) \quad \text{cl}(P(\psi)) = 1.$$

More precisely

$$(ii) \quad (x|\psi)\mathcal{O} = P(\psi)$$

and hence also

$$(iii) \quad ((x|\psi)^f) = a(\psi).$$

(ii) is obvious and (i) and (iii) are its immediate consequences.

Now let  $\Gamma$  be the Galois group of  $K$  over some subfield  $k$ .  $\Gamma$  will act on  $\mu_f$ , as a subgroup of  $K^*$ , and on  $\Omega_f$  by conjugation, and we have

$$(3.6) \quad \langle a^{\gamma}, \omega^{\gamma} \rangle = \langle a, \omega \rangle^{\gamma}.$$



Let  $u: \Gamma \rightarrow (\mathbb{Z}/f\mathbb{Z})^*$  be the homomorphism given by the action on  $\mu_f$ , i.e., defined by

$$(3.7) \quad {}^\gamma u(\gamma) = w \quad \text{for all } w \in \mu_f.$$

We define an involutory bijection  $c \mapsto c^*$  of  $\text{Hom}(\Gamma, (\mathbb{Z}/f\mathbb{Z})^*)$  onto itself by

$$c(\gamma) c^*(\gamma) = u(\gamma) \quad \text{for all } c, \quad \text{all } \gamma.$$

Let  $g, c \in \text{Hom}(\Gamma, (\mathbb{Z}/f\mathbb{Z})^*)$  and let  $t: \Gamma \rightarrow \mathbb{Z}$  satisfy

$$(3.8) \quad c(\gamma) = t(\gamma) \bmod f, \quad \text{for all } \gamma.$$

Suppose that  $g = c^*$ . Then the following conditions on  $a \in K^*$  are equivalent

$$(3.9a) \quad \langle a, {}^\gamma g(\gamma) \rangle = \langle a, \omega \rangle, \quad \text{for all } \gamma, \quad \text{all } \omega,$$

$$(3.9b) \quad \langle a, {}^\gamma t(\gamma) \rangle, \omega = \langle a, \omega \rangle, \quad \text{for all } \gamma, \quad \text{all } \omega,$$

$$(3.9c) \quad a^{{}^\gamma t(\gamma)-1} \in K^{*f}, \quad \text{for all } \gamma.$$

Moreover  $K(a^{1/f})/k$  is normal, if and only if (3.9a) holds for some  $g$ , and if and only if (3.9b), i.e., (3.9c) holds for some  $c$ , with  $t$  defined as in (3.8). Finally, in addition,  $\text{Gal}(K(a^{1/f})/K)$  will actually lie in the centre of  $\text{Gal}(K(a^{1/f})/k)$  precisely when  $g = 1$ , i.e. when  $c = u$ , as defined by (3.7).

Now assume  $c: \Gamma \rightarrow (\mathbb{Z}/f\mathbb{Z})^*$  is a surjective homomorphism, fixed once and for all. We shall then adopt the notation of §2, and in (3.8) take  $t = t_f$ . Let  $G_c$  be the subgroup of  $K^*$  of elements  $a$  satisfying (3.9).

Proposition. Let  $a \in G_c$  and  $\rho \in \mathbb{Z}(\Gamma)$ ,  $\rho \theta_f \in \mathbb{Z}(\Gamma/\text{Ker } c)$ .

Then

$$a^\rho \in K^{*f}.$$

Proof By Lemma 3,  $\rho$  lies in  $E$ , the  $\mathbb{Z}$ -module generated by  $f$  and by the  $\gamma t_f(\gamma) - 1$ . But for these particular values of  $\rho$ , we have  $a^\rho \in K^{*f}$  by definition.

Recall now the ideal equation (3.4), with  $a \in G_c$ . We see that, for all  $\gamma$ ,

$$a(\psi)^{\gamma t_f(\gamma) - 1} = f\text{-th power of an ideal.}$$

Hence, by Lemma 2, we now get

$$(3.10) \quad a(\psi) = \prod_{1 < d | f} a(\psi, d)^{f \theta_d},$$

where

$$(3.11) \quad \left\{ \begin{array}{l} \text{(i)} \quad a(\psi, d) \text{ is a square free integral ideal} \\ \quad \text{fixed under Ker } c_d, \\ \text{(ii)} \quad (a(\psi, d), a(\psi, e)^\gamma) = 1, \text{ for all } \gamma, \\ \quad \text{whenever } d \neq e, \\ \text{(iii)} \quad (a(\psi, d)^\gamma, a(\psi, d)^\delta) = 1, \text{ for } \gamma, \\ \quad \delta \in \Gamma/\text{Ker } c_d, \quad \gamma \neq \delta. \end{array} \right.$$

From the Proposition we now have the

Corollary. Let  $a \in G_c$ , corresponding to  $\psi$ , with (3.4), (3.10), (3.11) defining the ideals  $a(\psi, d)$ . Let  $\rho \in \mathbb{Z}(\Gamma)$ ,  $\rho \theta_f \in \mathbb{Z}(\Gamma/\text{Ker } c)$ . Then

$$\prod_{1 < d | f} \text{cl}(a(\psi, d))^{\rho \theta_d} = \text{cl}(P(\psi))^{\rho}.$$

Indeed by the Proposition

$$(a^\rho) = (b^f), \quad b \in K^*,$$

while by (3.4), (3.10)

$$(a^\rho) = \left( \prod_{1 < d | f} a(\psi, d)^{\rho \theta_d} \cdot b^{-\rho} \right)^f.$$

By Lemma 3,  $\rho \theta_d \in \mathbb{Z}(\Gamma)$ , and indeed

$$\prod_{1 < d | f} a(\psi, d)^{\rho \theta_d} b^{-\rho} = (b)$$

is principal.

1<sup>st</sup> Application. With  $\rho$  as above and  $\psi$  non-ramified,

$$\text{cl}(P(\psi))^{\rho} = 1.$$

The next application is Stickelberger's theorem.

#### §4. The Stickelberger relations

Let  $K$  now be the field of  $f$ -th roots of unity and  $k = Q$ . Take  $c = u$ :  $\Gamma \cong (\mathbb{Z}/f\mathbb{Z})^*$ , with  $u$  as in (3.7). We have to show that

$$(4.1) \quad c^{\rho \theta_f} = 1$$

for every ideal class  $C$  of  $K$  with  $\rho$  as before. Let  $p$  be a prime number  $\equiv 1 \pmod{f}$  having one of its prime divisors in  $C$ . Then  $Q(\mu_p)$  has a subfield  $L$  of degree  $f$  over  $Q$ , and the field  $N = LK$  has the form  $N = K(a^{1/f})$  with  $a \in G_C$ . As  $p$  is totally ramified of ramification index  $f$  in  $L$ , and non-ramified in  $K$ , its prime divisors in  $K$  are totally ramified of ramification index  $f$  in  $N$ . Moreover no other prime ideal is ramified in  $N/K$ , as no prime other than  $p$  is ramified in  $L/Q$ . All this implies, for  $\psi$  corresponding to  $a$ , that

$$(4.2) \quad \begin{cases} a(\psi, f) = p, & \text{a prime divisor of } p \\ a(\psi, d) = 1, & \text{for } d \neq f. \end{cases}$$

On the other hand,  $e^{2\pi i/p}$  generates a normal integral basis of  $L/Q$  (Hilbert), and thus also a normal integral basis of

$N/K$ , as  $L$  and  $K$  have coprime discriminants. By Lemma 5(i),  $\text{cl}(P(\psi)) = 1$ . By (4.2) and the Corollary in §3,  $\text{cl}(p)^{\rho \theta_f} = 1$ . But  $C = \text{cl}(p)^\gamma$  for some  $\gamma$ . Thus (4.1) will hold.

We can actually say more. By Lemma 5,  $a(\psi) = ((e^{2\pi i/p}/\psi)^f)$ . But  $(e^{2\pi i/p}/\psi) = \tau(\psi)$  is the Gauss sum.

Thus by (4.2), (3.10) we get

$$(4.3) \quad (\tau(\psi)^f) = p^{f \theta_f},$$

which is Stickelberger's prime decomposition rule for Gauss sums of prime fields.

#### §5. A cohomological criterion

We return to the general situation considered in §3 with  $c$  fixed, surjective. The proposition, in conjunction with (3.4), (3.10), (3.11) leads one to consider families  $\{a_d, b\}$  of fractional ideals in  $K$ , with  $1 < d|f$ , where

- (i) For each  $d$ ,  $a_d$  is a square free integral ideal, fixed under  $\text{Ker } c_d$ , and for  $\gamma, \delta \in \Gamma/\text{Ker } c_d$ , and  $\gamma \neq \delta$ , also  $(a_d^\gamma, a_d^\delta) = 1$ .
- (ii) If  $d \neq e$ , then  $(a_d^\gamma, a_e^\gamma) = 1$  for all  $\gamma$ .
- (iii) Whenever  $\rho \theta_f \in \mathbb{Z}(\Gamma/\text{Ker } c)$ ,  $\rho \in \mathbb{Z}(\Gamma)$ , then  $\prod_d a_d^{\rho \theta_d} b^{-\rho}$  is principal in  $K$ .

Denote by  $S_c$  the set of these families. If  $a \in G_c$  we obtain via (3.4) (3.10) such a family, with  $a_d = a(\psi, d)$ .

We thus have a map

$$s_c: G_c \rightarrow S_c, \quad ,$$

whose image we wish to characterise.

Let  $Y$  be the group of global units in  $K$ , and write  $H = Y/Y^f$ . Make  $H$  into a  $\Gamma$ -module, not in the obvious way, but twisted by  $c$ , i.e., so that if  $\eta \in Y$ ,  $y \in H$  its class then  $y^\gamma = \text{class of } \eta^{\gamma^{t_f(\gamma)-1}}$ .

If now  $\{a_f, b\} \in S_c$ , choose  $a \in K^*$  and for each  $\gamma$ , also  $b_\gamma \in K^*$ , so that

$$(a) = \prod_d a_d^{f \theta_d} b^{-f}$$

$$(b_\gamma) = \prod_d a_d^{(\gamma^{t_f(\gamma)-1}) \theta_d} b_\gamma^{-(\gamma^{t_f(\gamma)-1})}, \text{ for all } \gamma.$$

Then, for all  $\gamma$ ,

$$a^{\gamma^{t_f(\gamma)-1}} b_\gamma^{-f} = \eta(\gamma) \in Y.$$

Write

$$y(\gamma) = \text{class of } \eta(\gamma) \text{ mod } Y^f, \quad y(\gamma) \in H.$$

Then one verifies

I.  $y$  is a 1-cocycle of  $\Gamma$  in  $H$ ,

II. Its cohomology class only depends on  $\{a_d, b\}$ ,

not on  $a$  or  $b_\gamma$ . Denote it by  $h_c(\{a_d, b\})$ .

III.  $\text{Im } s_c = \text{Ker } h_c.$

Corollary. If  $(\text{order}(\Gamma), f) = 1$  then  $s_c$  is surjective.

#### REFERENCES

1. J. Coates,  $p$ -adic L-functions and Iwasawa's theory, Durham Symposium.
2. J. Cougnard, Propriétés galoisiennes des anneaux d'entiers des  $p$ -extension, to appear.
3. J. Cougnard, Un Contre-Exemple a une conjecture de J. Martinet, Durham Symposium.
4. A. Fröhlich, Galois Module Structure, Durham Symposium.
5. Leon R. McCulloh, A Stickelberger Condition on Galois module structure for Kummer extensions of prime degree. Durham Symposium.





## Fields of class two and Galois cohomology

H. Koch

In this lecture we describe the connection between three old results: A paper of A. Fröhlich on "fields of class two", in 1954 ([5]), the talk by J.R. Shafarevich at the International Congress of Mathematics in Stockholm 1962 on "algebraic number fields" ([18]) and the talk by J. Tate at the same congress about "duality in the Galois cohomology over number fields" ([20]).

The proofs for Shafarevich's results we are considering were published later ([19]), but the proofs for the results of Tate (which were given in less generality at the same time by Poitou [14]) were published only in part by several authors [7], [8].

In fact K. Haberland [6] recently gave detailed proofs of all the statements of Tate's Stockholm talk about Galois cohomology over number fields except the assertions about strict cohomological dimension in the case of restricted

ramification. Later A. Brumer pointed out that this question is related to the deep and unsolved problem of the non vanishing of the  $p$ -adic regulator (see Haberland [6], where one finds also a proof of the fact that  $H^3(\Omega_k, \mathbb{Z}) = \{0\}$  for the Galois group  $\Omega_k$  of the algebraic closure of a number field  $k$ , which played a role in the lectures of J.P. Serre and J. Tate at this conference).

1. Let us start by describing in brief these three results so far as they are relevant to the purposes of this lecture.

We use the following notations.  $p$  is a fixed rational prime,  $k$  an algebraic number field,  $S$  a set of places of  $k$ .  $k_S$  (respectively  $k_S(p)$ ), denotes the maximal algebraic extension (the maximal  $p$ -extension) of  $k$  which is unramified outside  $S$ . The Galois group  $G_S$  (respectively  $G_S(p)$ ) of the normal and in general infinite extension  $k_S/k$  (respectively  $k_S(p)/k$ ) is a topological group with Krull topology. The fixed field  $k_S^{(2)}(p)$  of the subgroup  $[[G_S(p), G_S(p)], G_S(p)]$  of  $G_S(p)$  is a "field of class two" in the terminology of Fröhlich, the Galois group  $G_S^{(2)}(p)$  of  $k_S^{(2)}(p)/k$  is of course a pro- $p$ -group of nilpotence class 2.

The philosophy is to consider the group theoretical structure of  $G_S$  respectively  $G_S(p)$ , respectively  $G_S^{(2)}(p)$  and to get in this way, via Galois theory, information about the set of all extensions of corresponding type.

Fröhlich's result is the determination of the group theoretical structure of  $G = G_S^{(2)}(p)$  together with its ramification subgroups in the case of a rational base field  $k = \mathbb{Q}$ . For the sake of simplicity we assume in the following  $p \neq 2$ .

If  $p \neq 2$ , then ramified places in a  $p$ -extension of  $\mathbb{Q}$  are primes  $q$  of the form  $q \equiv 1 \pmod{p}$  or  $q = p$ . So we assume that  $S$  contains only places of this type.

Let  $q$  be a fixed prime divisor of  $\mathbb{Q}_S^{(2)}(p)$  above  $q$  and let  $\tau_q$  be a generator of the inertia group  $I_q$  of  $q$  as normal subgroup of the decomposition group  $D_q$  (in fact,  $I_q$  is cyclic for  $q \neq p$ ). Then  $\{\tau_q/q \in S\}$  is a minimal generator system of  $G$  and the relations

$$\tau_q^{q-1}(\tau_q, \sigma_q) = 1 \quad \text{for } q \in S, \quad q \neq p \quad (1)$$

form together with the universal relation  $[[G, G], G] = \{1\}$  a generating relation system of  $G$ . Here  $\sigma_q$  is an extension in  $D_q$  of the Frobenius automorphism of  $q$  in  $D_q/I_q$

and  $(\tau_q, \sigma_q)$  denotes the commutator  $\tau_q \sigma_q \tau_q^{-1} \sigma_q^{-1}$ . The automorphism  $\sigma_q$  is determined, by class field theory, over  $\mathbb{Q}$  up to commutators. But  $\sigma_q$  stands in (1) already in a commutator, i.e.,  $(\tau_q, \sigma_q)$  is determined up to commutators of weight three which are in the universal relation  $[[G, G], G] = \{1\}$ . This means that we have determined the structure of  $G$  (and the inertia subgroups  $I_q$ ) completely. From the result of Fröhlich we see that we know the set of fields of class two over the rationals very well.

The paper of Shafarevich dealt with the general case of an algebraic number field  $k$  as base field and he was interested in the structure of  $G_S(p)$ . Two fundamental invariants of  $G_S(p)$  are its generator rank  $d$  and its relation rank  $r$ .

The generator rank  $d$  can be computed by means of class field theory over the base field  $k$ , and it can therefore be considered as known. The result of Shafarevich consists in an estimate of  $r$  from above for finite  $S$ :

$$r \leq d - 1 - \sum [k_p : \mathbb{Q}_p] + r_1 + r_2 + \theta(k, S), \quad (2)$$

where the sum is to be taken over all places  $p$  in  $S$  which lie above  $p$ ,  $r_1$  is the number of real conjugates and  $r_2$  half

of the number of complex conjugates of  $k$ .  $\theta(k, S) = 1$  if the group  $\mu_p$  of the  $p$ th roots of unity is contained in  $k$  and  $S$  is empty,  $\theta(k, S) = 0$  otherwise.

Concerning the duality theorem of Tate we mention here only a special case which we need for the following. We assume that all places of  $k$  above  $p$  are in  $S$ . Let  $\bar{k}_p$  be the algebraic closure of  $k_p$  and  $G_p = \text{Gal}(\bar{k}_p/k_p)$ .

The noncanonical inclusion  $k_S \subset \bar{k}_p$  induces a non-canonical map  $\phi_p : G_p \rightarrow G_S$ , which induces canonical maps of the cohomology groups.

$$H^i(G_S, M) \xrightarrow{\phi_p^*} H^i(G_p, M).$$

Here  $M$  is a  $G_S$ -module, but we are only interested in the cases where  $M = \mathbb{Z}/p\mathbb{Z}$  and  $G_S$  acts trivially, or where  $M = \mu_p \subset k_S$  the group of  $p$ -th roots of unity. Let  $\text{Ker } H^i(G_S, M)$  be the kernel of the map

$$\Pi \phi_p^* : H^i(G_S, M) \rightarrow H^i(G_p, M).$$

Then there is a natural exact sequence

$$\begin{aligned} 0 \rightarrow \text{Ker } H^1(G_S, \mu_p)^* \rightarrow H^2(G_S, \mathbb{Z}/p\mathbb{Z}) \rightarrow \sum_{p \in S} H^2(G_p, \mathbb{Z}/p\mathbb{Z}) \rightarrow \\ \rightarrow H^0(G_S, \mu_p)^* \rightarrow 0. \end{aligned} \quad (3)$$

The groups  $\text{Ker } {}^1(G_S, \mu_p)$  and  $H^0(G_S, \mu_p)$  are finite and the star denotes the dual abelian group.

2. Now we are going to make a common picture out of the three mentioned theorems. We start with a group theoretical principle which is a generalisation of Tate's characterisation of the relation rank of a pro-p-group.

Assume we have pro-p-groups  $G, G_i$ , where  $i$  runs through an index set  $I$ , and a family of morphisms

$$G_i \xrightarrow{\phi_i} G.$$

We consider the representations

$$\begin{array}{ccccc} R_i & \longrightarrow & F_i & \longrightarrow & G_i \\ \downarrow \psi_i & & \downarrow \psi_i & & \downarrow \phi_i \\ R & \longrightarrow & F & \longrightarrow & G \end{array} \quad (4)$$

of  $G_i, G$  by free pro-p-groups  $F_i, F$  with the same generator rank as  $G_i, G$  and the relation modules  $R_i, R$ . The morphisms  $\psi_i$  are chosen such that the diagram (4) commutes.

Let  $\{\rho_1, \dots, \rho_s\}$  be a minimal set of elements of  $R$  with the property that they together with  $\psi_i(R_i)$ , for  $i \in I$ , generate  $R$  as normal closed subgroup of  $F$ . The  $\phi_i$  induce a



map

$$\phi^* : H^2(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow \prod_{i \in I} H^2(G_i, \mathbb{Z}/p\mathbb{Z}).$$

Then

$$\dim_{\mathbb{Z}/p\mathbb{Z}} \text{Ker } \phi^* = s. \quad (5)$$

In other words: we describe  $G$  by the help of two sorts of relations: the  $\rho_1, \dots, \rho_s$ , which we call the unknown relations, and the relations in  $\psi_i(R_i)$ , which come from the groups  $G_i$ . We call them the known relations. If  $\phi^*$  is injective, all relations are known. If  $I$  is empty, we have the usual characterisation of the relation rank by Tate. One finds the proof of (3) in H. Koch [9], Satz 6.11, it is based on the proof of proposition I.27 in J.P. Serre [16].

Now we go over to our field theoretical situation. Our family of morphisms is  $\phi_p : G_p(p) \rightarrow G_S(p)$ ,  $p \in S$ .

We are interested in the group theoretical description of  $G_S(p)$ . Consider first the local groups  $G_p(p) = G$ . Here the structure is well known.

If the characteristic  $\chi(p)$  of the residue class field of  $k_p$  is  $\neq p$  and  $\mu_p \not\subset k_p$ , the extension  $\bar{k}_p/k_p$  is unramified and  $G$  is canonically isomorphic to  $\mathbb{Z}_p$ . If  $\chi(p) = p$  and  $\mu_p \subset k_p$ , the group  $G$  is generated by two elements  $\tau_p, \sigma_p$  which are connected by a single relation of the form

$\tau_p^{N(p)-1}(\tau_p, \sigma_p) = 1$ , where  $\tau_p$  is a generator of the inertia group of  $\bar{k}_p/k_p$  and  $\sigma_p$  is an extension of the Frobenius automorphism of the maximal unramified subextension to  $\bar{k}_p$ .

The next case is  $\chi(p) = p$ ,  $\mu_p \not\subset k_p$ . Then  $G$  is a free pro- $p$ -group with  $[k_p : \mathbb{Q}] + 1$  generators. We can choose  $\sigma_p$  as one generator and the others out of the inertia group. There are several proofs of this result, but the most elegant is the following version of the initial proof of Shafarevich [17].

From local class field theory it follows that

$$1 - d(G) = \dim H^0(G, \mathbb{Z}/p\mathbb{Z}) - \dim H^1(G, \mathbb{Z}/p\mathbb{Z}) = -[k_p : \mathbb{Q}_p],$$

where  $d(G)$  is the generator rank of  $G$ . Let  $H$  be an open subgroup of  $G$  with fixed field  $L$ . Then

$$1 - d(H) = -[L : \mathbb{Q}] = (1 - d(G)) [G : H].$$

We see that the partial Euler Poincaré characteristic

$1 - d(G)$  is multiplicative for open subgroups. Hence it is the full Euler Poincaré characteristic and  $G$  has cohomological dimension 1, i.e.,  $G$  is a free pro- $p$ -group.

The most complicated case is  $\chi(p) = p$ . Then  $G$  is a pro- $p$ -group with generator rank  $[k_p : \mathbb{Q}] + 2$  and relation rank 1.  $G$  is a Poincaré group of cohomological dimension 2.

These groups were fully described and classified by Demushkin [3], [4], [4a] with contributions by J.P. Serre [15] and J. Labute [12]. For our purposes we need indeed something more arithmetical, because we are mainly interested in global fields, for details see H. Koch [9], §10.3.

The last case is  $k_p = \mathbb{R}$  or  $\mathbb{C}$  with  $G$  cyclic of order 1 or 2. This case plays a role of course only for  $p = 2$ .

Now we have the "known relations" of  $G_S(p)$  and the question is whether there are still unknown relations. For this one has to examine the kernel  $S_S$  of the localisation map

$$H^2(G_S(p), \mathbb{Z}/p\mathbb{Z}) \rightarrow \prod_{p \in S} H^2(G_p(p), \mathbb{Z}/p\mathbb{Z}).$$

One can give an estimation of  $S_S$ . Namely, there is a canonical injection of  $S_S$  into  $B_S = (V_S/k^{\times p})^*$ , where  $V_S$  is the following subgroup of  $k^{\times}$ :

$$V_S = \{\alpha \in k^{\times} \mid (\alpha) = a^p, \alpha \in k_p^p \text{ for } p \in S\}.$$

For the proof see H. Koch [9] §11.2.

3. Now we return to the result of Fröhlich which was mentioned at the beginning of this talk. Let  $k = \mathbb{Q}$  and  $p \neq 2$ .

Then obviously  $B_S = \{0\}$  for any  $S$ . So we have only known relations and they are exactly of the form of Fröhlich's relation.

Let us consider the situation more closely. We denote the image of  $\tau_q$  under  $\phi_q$  again by  $\tau_q$ . Then  $\{\tau_q \mid q \in S\}$  is a minimal set of generators of  $G_S(p)$  if we assume that  $S$  contains only primes  $q$  of the form  $q \equiv 1 \pmod{p}$  or  $q = p$ . For each  $q \in S$ , the group  $G_q(p)$  has two generators  $\tau_q, \sigma_q$  so that we have to consider the free pro- $p$ -group  $F_q$ , respectively  $F$ , with generators  $t_q, s_q$  for  $q \in S$ , respectively  $\{t_q \mid q \in S\}$ . Now we have to construct the map  $\psi_q$ :

$$\begin{array}{ccc}
 (t_q, s_q) & \longrightarrow & (\tau_q, \sigma_q) \\
 \downarrow \psi_q & & \downarrow \phi_q \\
 (t_q \mid q \in S) & \longrightarrow & (\tau_q \mid q \in S)
 \end{array}$$

Clearly we may set  $\psi_q t_q = t_q$ , but the image of  $s_q$  is given by class field theory over  $\mathbb{Q}$  only up to commutators:

$$\phi_q(\sigma_q) \equiv \prod_{q' \in S} \tau_{q'}^{a_{q'q}} \pmod{[G_S(p), G_S(p)]},$$

$$\psi_q(s_q) \equiv \prod_{q' \in S} t_{q'}^{a_{q'q}} \pmod{[F, F]}.$$

The relations are of the form

$$\rho_q = t_q^{q-1}(q_q, s_q)$$

for  $q \in S$ ,  $q \neq p$ . Hence we have them determined, by class field theory over  $\mathbb{Q}$ , up to commutators of weight 3 and that includes the result of Fröhlich.

It is clear how the result of Fröhlich generalizes to arbitrary number fields.

4. One gets Shafarevich's estimate (2) for the relation rank  $r$  of  $G_S(p)$  from the above estimate of  $S_S$ . In fact, we have for finite  $S$

$$r = \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(G_S(p), \mathbb{Z}/p\mathbb{Z}) \leq \dim_{\mathbb{Z}/p\mathbb{Z}} B_S$$

$$+ \sum_{z \in S} \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(G_z(p), \mathbb{Z}/p\mathbb{Z}). \quad (6)$$

It follows from Hasse's local global principle that we can in the last sum ignore one place  $z$  if  $\mu_p \subset k$ . Class field theory computation gives on the other hand for the generator rank  $d$  of  $G_S(p)$

$$d = \sum_{\substack{z \in S \\ z/p}} [k_z : \mathbb{Q}_p] - \delta(k) - r_1 - r_2 + 1 + \sum_{z \in S} \delta(k_z) + \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{B}_S, \quad (7)$$

where  $\delta(L)$ , for a field  $L$ , is one if  $\mu_p \subset L$  and zero otherwise. It follows from our above consideration of  $G_Z(p)$  that

$$\dim_{\mathbb{Z}/p\mathbb{Z}} H^2(G_Z(p), \mathbb{Z}/p\mathbb{Z}) = \delta(k_z).$$

This together with (6) and (7) gives Shafarevich's estimate (2).

5. What is the meaning of Tate's sequence (3) in this connection?

One can prove  $H^2(G_S, \mathbb{Z}/p\mathbb{Z}) \cong H^2(G_S(p), \mathbb{Z}/p\mathbb{Z})$  and the same for the local groups. This was done by O. Neumann [13] and K. Haberland [6]. It is easy to see that  $\text{Ker}^1(G_S, \mu_p)^*$  can be identified with  $\mathcal{B}_S$ . This gives in the case  $z \in S$  for  $\mathbb{Z}/p$  in conjunction with (3) the exact sequence

$$\begin{aligned} 0 \rightarrow \mathcal{B}_S \rightarrow H^2(G_S(p), \mathbb{Z}/p\mathbb{Z}) \rightarrow \sum_{z \in S} H^2(G_Z(p), \mathbb{Z}/p\mathbb{Z}) \rightarrow \\ \rightarrow H^0(G_S, \mu_p)^* \rightarrow 0 \end{aligned}$$

which means that we have equality in Shafarevich's estimate.

For  $\mu_p \subset k$ , this was first proved by A. Brumer [2] in 1966. For  $\mu_p \not\subset k$ , this was first proved by O. Neumann [13] in 1975. His proof is independent of Tate's duality theorem.

In general in the same way as in the  $p$ -situation one can prove that there is a natural embedding of  $\text{Ker}^2(G_S, \mathbb{Z}/p\mathbb{Z})$  into  $B_S$ . This can be considered as a generalisation of Tate's duality theorem in the special case  $M = \mathbb{Z}/p\mathbb{Z}$ . But it seems to be impossible to understand  $B_S$  as dual to the kernel  $\text{Ker}^1$  for some  $G_S$ -module.

6. We finish with two remarks.

a) Consider the cokernel  $C_S$  of the map

$$\text{Ker}^2(G_S(p), \mathbb{Z}/p\mathbb{Z}) \rightarrow B_S.$$

The dual  $C_S^*$  is a subgroup of  $V_S/k^{\times p}$ . It is possible to compute  $C_S^*$  as a group of universal norms in  $k \pmod{k^{\times p}}$ .

For details see H. Koch [10].

b) Another approach to the questions considered in this talk goes back to J.P. Serre [16], I.4.4, and was



developed by L.W. Kuzmin [11].

His main result is the equation

$$r(G_S(p)) = d(G_S(p)) - \text{rk}(G_S(p)/[G_S(p), G_S(p)]) \\ + d(M(G_S(p)))$$

with a computation of the Schur multiplier  $M(G_S(p))$  by means of universal norms of some idèles. Kuzmin assumes that no archimedean primes are in  $S$ .

This result looks rather complicated, but Kuzmin was able to deduce from it that the cohomological dimension of  $G_S(p)$  is less than or equal to two in the case when the prime divisors of  $p$  are in  $S$  and the ground field  $k$  is totally imaginary if  $p = 2$ .

#### REFERENCES

1. M.I. Bashmakov, Cohomology of Abelian manifolds, Usp. Mat. nauk XXVII 6 (1972) (in Russian) 25-66.
2. A. Brumer, Galois groups of extensions of algebraic number fields with given ramification, Mich. Math. J., 13 (1966), 33-40.
3. S.P. Demushkin, The maximal  $p$ -extension of a local field, Izv. AN SSSR 25 (1961), 329-346, (in Russian).
4. S.P. Demushkin, On 2-extensions of local fields, Sibirsk. matem. J. 4 (1963), 951-955 (in Russian).

- 4a. S.P. Demushkin, Topological 2-groups with even number of generators and one complete defining relation, *Izv. AN SSSR* 29 (1965), 3-10 (in Russian).
5. A. Fröhlich, On Fields of Class Two, *Proc. London Math. Soc.* (3) 4 (1954), 235-256.
6. K. Haberland, Dissertation, Berlin 1975.
7. K. Höchsmann, Zum Einbettungsproblem, *J. reine angew. Math.*, 229 (1968), 81-106.
8. B. Kazornovski, Appendix to [1].
9. H. Koch, *Galoissche Theorie der p-Erweiterungen*, Berlin 1970.
10. H. Koch, Zur Galoisschen Theorie der maximalen p-Erweiterungen mit vorgegebener Verzweigungsstellen, *Math. Nachr.* 61 (1974) 47-50.
11. W. Kuzmin, Homology of profinite groups, Schur multiplier and class field theory, *Izv. AN SSSR* 33 (1969), 1220-1254 (in Russian).
12. J. Labute, Classification of Demushkin groups, *Can. J. Math.* 19 (1966), 106-132.
13. O. Neumann, On p-closed algebraic number fields with restricted ramification, *Izv. AN SSSR* 39 (1975), 259-271 (in Russian) (see also "Durham").
14. G. Poitou, *Seminaire de Lille* 1962-63.
15. J.P. Serre, Structure de certains pro-p-groups *Sem. Bourbaki* 1962-1963, exposé 252.
16. J.P. Serre, *Cohomologie Galoisienne*, Springer Lecture Notes 5, Berlin 1964.
17. I.R. Shafarevich, On p-extensions, *Mat. sbor.* 20 (1947), 351-363.

18. I.R. Shafarevich, Algebraic Number fields (in Russian) Proc. I.C.M. 1962, 163-176.
19. I.R. Shafarevich, Extensions with prescribed ramification points, (Russian with French summary) Publ. Math. I.H.E.S. 18 (1963).
20. J. Tate, Duality Theorems in Galois Cohomology over Number fields, Proc. I.C.M. 1962, 288-295.

On  $p$ -closed number fields and an analogue of Riemann's  
existence theorem

Olaf Neumann

This note is an account of some recent work on  $p$ -closed number fields with restricted ramification. The main reference is the paper [13].

Let  $F$  be any field. Denote by  $\bar{F}$  a separable algebraic closure of  $F$  and by  $\text{Gal}(K/F)$  the Galois group of a Galois extension  $K/F$ . We will use the abbreviation  $H^i(K/F, A)$  for the cohomology groups  $H^i(\text{Gal}(K/F), A)$ .

Let  $k$  be a finite algebraic number field,  $S$  any set of primes of  $k$ . Denote by  $k_S$  the maximal Galois extension of  $k$  unramified outside  $S$  (= union of all finite Galois extensions with ramification points only in  $S$ ). If  $p$  is a fixed rational prime then the notion " $p$ -extension" will be used in the sense of "normal extension of  $p$ -power degree". A normal extension  $K/k$  is called  $(S, p)$ -closed if  $K$  is contained in  $k_S$  and if there is no cyclic extension  $L/K$  of degree  $p$  with

$L \subseteq k_S$ . Obviously, this is equivalent to  $H^1(k_S/K, \mathbb{Z}/p\mathbb{Z}) = 0$ . The smallest  $(S, p)$ -closed extension of  $k$  is just the maximal  $p$ -extension  $k_S(p)/k$  of  $k$  unramified outside  $S$ .

For any field  $F$ , the symbol  $\delta(F)$  (with respect to  $p$ ) takes the value 1 if  $F$  contains the  $p$ -th roots of unity and is 0 otherwise.

### §1. The main results

Let  $p$  be a rational prime and let  $S_0$  be the set of primes of  $k$  consisting of all archimedean primes and all primes lying over  $p$ .

Theorem 1 ([13], theorem and corollary 1). Let  $S$  be any set of primes in  $k$  with  $S \supseteq S_0$ ,  $K/k$  any  $(S, p)$ -closed extension. Then the following statements hold.

a) Let  $A$  be a  $p$ -primary finite  $\text{Gal}(K/k)$ -module. Then the inflation maps

$$H^i(K/k, A) \rightarrow H^i(k_S/k, A) \quad (i \geq 0) \quad (1.1)$$

are isomorphisms.

b) The cohomological  $p$ -dimension of the group  $\text{Gal}(K/k)$  is  $\leq 2$ :

$$\text{cd}_p \text{Gal}(K/k) \leq 2, \quad (1.2)$$

i.e., under the assumptions of a) we have

$$H^i(K/k, A) = 0 \quad \text{for } i \geq 3.$$

(For  $p = 2$  we must assume that  $k$  is totally imaginary.)

c) There exists an exact sequence

$$\begin{aligned} 0 \rightarrow B_S \rightarrow H^2(K/k, \mathbb{Z}/p\mathbb{Z}) &\xrightarrow{\lambda} \sum_{p \in S} H^2(\bar{k}_p/k_p, \mathbb{Z}/p\mathbb{Z}) \\ &\rightarrow G \rightarrow 0 \end{aligned} \quad (1.3)$$

where  $k_p$  denotes the  $p$ -adic completion of  $k$  and where  $\lambda$  is the localization map induced by homomorphisms  $\text{Gal}(\bar{k}_p/k_p) \rightarrow \text{Gal}(K/k)$ .  $B_S$  is defined as the dual space of  $V_S/k^{\times p}$  where

$$V_S = \{\alpha \in k^{\times} \mid (\alpha) = a^p, \alpha \in k_p^{\times p} \text{ for } p \in S\}$$

The group  $G$  is isomorphic to  $\mathbb{Z}/p\mathbb{Z}$  if  $k$  contains the  $p$ -th roots of unity and  $= 0$  otherwise.

Theorem 2. Let  $S_1, S_2$  be sets of primes of  $k$  with

$S_2 \supseteq S_1 \supseteq S_0$ ,  $K_i/k$  ( $i = 1, 2$ ) be  $(S_i, p)$ -closed extensions with  $K_2 \supseteq K_1$ . Then

$$\text{a) } H^2(K_2/K_1, \mathbb{Z}/p\mathbb{Z}) = 0. \quad (1.4)$$

b) In particular, let  $K_2/K_1$  be a  $p$ -extension. Then the group  $\text{Gal}(K_2/K_1)$  is a free pro- $p$ -group and can be decomposed

into factors which correspond to the primes in  $S_2 \setminus S_1$ .

More precisely, let be  $p \in S_2 \setminus S_1$ ,  $P_1$  be a prime of  $K_1$  dividing  $p$ ,  $P_2$  be a prime of  $K_2$  dividing  $P_1$ . We choose for every  $P_1$  the inertia group  $T_{P_2}$  for some fixed prolongation  $P_2$  and define  $T_p$  to be the subgroup of  $\text{Gal}(K_2/K_1)$  generated by the chosen  $T_{P_2}$  where  $P_1$  varies over all primes of  $K_1$  dividing  $p$ . Then the canonical homomorphism of the free pro- $p$ -product  $\bigstar_{p \in S_2 \setminus S_1} T_p$  into  $\text{Gal}(K_2/K_1)$  is an isomorphism:

$$\text{Gal}(K_2/K_1) \stackrel{\sim}{=} \bigstar_{p \in S_2 \setminus S_1} T_p. \quad (1.5)$$

Moreover, the inertia group  $T_{P_2}$  of a prime  $P_2$  of  $K_2$  lying over a prime in  $S_2 \setminus S_1$  is either isomorphic to  $Z_p$  or to  $\{1\}$ :

$$T_{P_2} = \{1\} \quad \text{if } \delta(K_2, P_2) = 0 \quad (\Leftrightarrow \delta(K_1, P_1) = 0) \quad (1.6)$$

$$T_{P_2} \stackrel{\sim}{=} Z_p \quad \text{if } \delta(K_2, P_2) = 1 \quad (\Leftrightarrow \delta(K_1, P_1) = 1) \quad (1.7)$$

The isomorphism (1.5) is an analogue to Riemann's existence theorem which allows us to describe the groups  $\text{Gal}(k_S/k)$  for  $k$  = algebraic function field of one variable over  $\mathbb{C}$  (cf. Šafarevič [14]) as it follows from the "Freiheitssatz" by W. Magnus [9] that the fundamental group  $\pi_1(R \setminus S)$  where  $R$  is a compact Riemann surface contains a



free subgroup generated by elements corresponding to the ramification points in  $S$  if the genus of  $R$  is  $\geq 1$ . In the genus 0 case one must omit one element of  $S$ . Theorem 2 generalizes a theorem of J. Neukirch [11] (theorem 11.3) on  $p$ -extensions of  $\mathbb{Q}$ .

## §2. Proof of theorem 1 (sketch)

The main ingredients of the proof are an appropriate twisting of Galois modules and the cohomology of the group  $E_S$  of  $S$ -units in the field  $k_S$ . An element  $\alpha$ ,  $\alpha \in k_1^\times$ ,  $k_1/k$  finite, is called an  $S$ -unit if in the prime decomposition of the principal ideal  $(\alpha)$  only prime divisors lying over primes in  $S$  occur. For the cohomology of  $E_S$  refer to H. Koch [5], chap. 13 and to A. Brumer [1]. Statement b) can be deduced from a) together with well-known facts about  $k_S$  ([4], [3], [13]). Therefore, it suffices to derive a), which in turn follows (by the exact sequence of Hochschild-Serre) from this.

Key Lemma.  $H^2(k_S/K, \mathbb{Z}/p\mathbb{Z}) = 0$ .

In order to prove this lemma notice that  $K$  contains the

cyclotomic  $\mathbb{Z}_p$ -extension  $K_0/k$  for  $p \neq 2$  and  $K_0/k(\sqrt{-1})$  for  $p = 2$ . Let  $\mu_p^n$  denote the Galois module of the  $p^n$ -th roots of unity and let be  $K' = K(\mu_p)$ . Obviously,  $K'$  contains all roots of unity of  $p$ -power order. We denote by  $T$  the Tate module  $T = \varprojlim_p \mu_p^n$ .

Definition. Let  $X$  be any discrete  $p$ -primary  $\text{Gal}(K'/k)$ -module. Define the  $\text{Gal}(K'/k)$ -module  $X(-1)$  by  $X(-1) = \text{Hom}_{\mathbb{Z}_p}(T, X)$ . Then the correspondence

$$X \longmapsto [X(-1)]^{\text{Gal}(K'/K)} \stackrel{\text{Df}}{=} F(X)$$

defines an exact functor  $F$  into the category of discrete  $p$ -primary  $\text{Gal}(K/k)$ -modules.

The exactness of  $F$  is obvious by virtue of the exactness of the Tate twisting  $X \longmapsto X(-1)$  and the fact that  $p$  does not divide  $[K':K]$ .

Now one uses the  $p$ -divisibility of  $E_S$ , i.e., that the sequence

$$\{1\} \rightarrow \mu_p \rightarrow E_S \xrightarrow{p} E_S \rightarrow \{1\}$$

is exact. By class field theory one gets an isomorphism of  $\text{Gal}(K'/k)$  modules

$$X/pX \xrightarrow{\sim} H^2(k_S/K', \mu_p) \quad (2.1)$$

where  $X$  denotes the  $p$ -primary component of  $H^1(k_S/K', E_S)$ .

Since every isomorphism (of abelian groups)  $Z/pZ \xrightarrow{\sim} \mu_p$  yields an isomorphism

$$H^i(k_S/K, Z/pZ) \xrightarrow{\sim} F(H^i(k_S/K', \mu_p)) \quad (i \geq 0) \quad (2.2)$$

we derive by easy calculations using  $H^1(k_S/K, Z/pZ) = 0$  and the vanishing of the  $p$ -component of the Brauer group of  $K'$ :

$$F(X/pX) = 0. \quad (2.3)$$

Now (2.1) together with (2.2) and (2.3) gives us the key lemma.

The statement c) is deduced from class field theory again by using the functor  $F$ . The description of  $B_S = \text{Ker } \lambda$  arises from comparison of Kummer theory and properties of the Hilbert class field. It is clear that statement c) can also be derived immediately from statement a) and Tate's "long exact sequence" ([17], theorem 3.1; cf. [3]).

### § 3. Some corollaries of theorem 1 and bibliographical remarks

K. Haberland gave in his dissertation [3] an alternative

proof of statement a) of our theorem 1. A. Brumer [1] had proved theorem 1 under the assumption  $\mu_p \subset k$ .

It is well-known that for the  $p$ -extension  $k_S(p)/k$  the number

$$r(G_S(p)) = \dim_{\mathbb{F}_p} H^2(k_S(p)/k, \mathbb{Z}/p\mathbb{Z})$$

coincides with the minimal number of defining relations for the pro- $p$ -group  $G_S(p) = \text{Gal}(k_S(p)/k)$  (cf. [16], [5]). Now we can deduce from statement c) the exact size of  $r(G_S(p))$ :

Corollary 3.1. If  $S$  is finite then

$$r(G_S(p)) = \sum_{p \in S} \delta(k_p) - \delta(k) + \dim B_S. \quad (3.1)$$

I.R. Šafarevič had proved ([15]) that  $r(G_S(p))$  is not greater than the right-hand side of (3.1).

The estimate  $\text{cd}_p G_S(p) \leq 2$  was first proved by A. Brumer [1] (in the case  $\mu_p \subset k$ ) and by L.V. Kuz'min [7], [8] (in general).

H. Koch ([5], theorem 11.3 cf. [4]) stated that for arbitrary sets  $S$  (without our restrictions on  $S$ ) the kernel  $S_S$  of  $\lambda$  is canonically injected in  $B_S$ . Furthermore, in his paper [6] H. Koch described the quotient  $B_S/S_S$  in terms

of universal norms in the group  $V_S/k^{\times p}$  with respect to all finite intermediate extensions in  $k_S(p)/k$  (cf. [4]). Since we have in our case the equality  $S_S = B_S$ , we can derive immediately:

Corollary 3.2 Let  $V_S(L)$  be the group

$$V_S(L) = \{\alpha \in L^\times \mid (\alpha) = a^p, \alpha \in L^{\times p}_P \text{ for } P, P|p, p \in S\} \quad (3.2)$$

Then for any  $(S, p)$ -closed extension  $K/k$  one has

$$\bigcap_L \text{Norm}_{L/k} V_S(L) \cdot k^{\times p} = k^{\times p} \quad (3.3)$$

where  $L$  runs over all finite extensions  $L/k$  with  $K \supset L$ .

For Koch's theorem [6] tells us that (3.3) is certainly true if  $L$  ranges over all finite extensions in the smallest  $(S, p)$ -closed extension.

Let  $\text{scd}_p G$  denote the strict cohomological  $p$ -dimension of a profinite group  $G$ .

Corollary 3.3 Let  $k'/k$  be any finite extension with  $k' \subset k_S$  and let  $k'(p)$  denote the maximal  $p$ -extension of  $k'$  inside  $k_S$ . Then  $\text{scd}_p \text{Gal}(k_S/k) \leq 2 \iff$  For all  $k'$ :  $\text{scd}_p \text{Gal}(k'(p)/k') \leq 2$ .

Proof. Let  $U = \text{Gal}(k_S/k')$  be any open subgroup of  $G = \text{Gal}(k_S/k)$ . One has the chain of the following equivalent assertions:

$$\begin{aligned} \text{scd}_p G \leq 2 & \Leftrightarrow \forall U: H^3(U, \mathbb{Z})_p = 0 \\ & \Leftrightarrow \forall U: H^3(U, \mathbb{Z}_p) = 0 \\ & \Leftrightarrow \forall U: H^2(U, \mathbb{Q}_p/\mathbb{Z}_p) = 0 \\ & \Leftrightarrow \forall U: \varinjlim_n H^2(U, \frac{1}{p^n} \mathbb{Z}_p/\mathbb{Z}_p) = 0 \end{aligned}$$

But by the theorem 1 a) we know that

$$H^2(U, \frac{1}{p^n} \mathbb{Z}_p/\mathbb{Z}_p) \simeq H^2(k'(p)/k', \frac{1}{p^n} \mathbb{Z}_p/\mathbb{Z}_p)$$

From this we easily deduce corollary 3.3.

#### §4. Proof of theorem 2

Let  $S_1, S_2$  be sets of primes of  $k$  with  $S_2 \supseteq S_1 \supseteq S_0$ ,  $K_i/k$  ( $i = 1, 2$ ) be  $(S_i, p)$ -closed extensions with  $K_2 \supseteq K_1$ .

Let  $L$  be a finite extension of  $k$  with  $L \subset K_1$  and  $S_2(L)$  the set of primes of  $L$  lying over  $S_2$ . From (1.3) we obtain the exact sequence

$$\begin{aligned} 0 \rightarrow (V_{S_2}(L)/L^{\times p})^* & \rightarrow H^2(K_2/L, \mathbb{Z}/p\mathbb{Z}) \\ & \rightarrow \sum_{P \in S_2(L)} H^2(\overline{L_P}/L_P, \mathbb{Z}/p\mathbb{Z}) \end{aligned} \quad (4.1)$$

(where  $^*$  denotes the Pontrjagin dual). Taking inductive

limits over  $L$  with respect to the restriction maps we can use the isomorphisms

$$\lim_{\rightarrow} H^i(K_2/L, Z/pZ) \xrightarrow{\sim} H^i(K_2/K_1, Z/pZ) \quad (i \geq 0) \quad (4.2)$$

and

$$\begin{aligned} \lim_{\rightarrow} \sum_{P \in S_2(L)} H^i(\overline{L_P}/L_P, Z/pZ) \\ \xrightarrow{\sim} \prod_{P_1} H^i(\overline{K_{1,P_1}}/K_{1,P_1}, Z/pZ) \quad (i \geq 0) \end{aligned} \quad (4.3)$$

where  $P_1$  runs over all primes of  $K_1$  lying over primes of  $k$  in  $S_2$ . These isomorphisms arise immediately from the definition of Galois cohomology groups and their localization maps together with the trivial action of all groups in question on  $Z/pZ$ . The degree of  $K_{1,P_1}$  is divisible by  $p^\infty$  resp.  $K_{1,P_1} = \overline{K_{1,P_1}} = C$  for the archimedean  $P_1$  and  $p = 2$ . Hence we have

$$H^2(K_{1,P_1}/K_{1,P_1}, Z/pZ) = 0. \quad (4.4)$$

On the other hand, we see that

$$\lim_{\rightarrow} (V_{S_2}(L)/L^{\times p})^* = (\lim_{\leftarrow} V_{S_2}(L)/L^{\times p})^*$$

where the inverse limit is taken with respect to the norm maps. Obviously, the  $L$ -coordinate of each element of

$$\lim_{\leftarrow} V_{S_2}(L)/L^{\times p} \text{ belongs to } \left( \bigcap_M \text{Norm}_{M/L} V_{S_2}(M) \cdot L^{\times p} \right) / L^{\times p}$$



where  $M$  ranges over all finite extensions  $M/L$  with  $M \subset K_1$ . But, in virtue of  $V_{S_2}(M) \subseteq V_{S_1}(M)$ , it is easily deduced from corollary 3.2. that

$$\bigcap_M \text{Norm}_{M/L} V_{S_2}(M) \cdot L^{\times p} = L^{\times p}$$

This means that

$$\lim_{\rightarrow} (V_{S_2}(L)/L^{\times p})^* = \{1\}. \quad (4.5)$$

The sequence (4.1) remains exact after taking inductive limits. Thus theorem 2 a) follows directly from (4.2), (4.3), (4.4) and (4.5).

Suppose that  $K_2/K_1$  is a  $p$ -extension. The assertion  $H^2(K_2/K_1, \mathbb{Z}/p\mathbb{Z}) = 0$  amounts to saying that  $\text{Gal}(K_2/K_1)$  is a free pro- $p$ -group (cf. [16], [5]). To prove the finer statements about  $\text{Gal}(K_2/K_1)$  it will be enough to prove them for the maximal  $p$ -extension  $\overline{K_1}(p)/K_1$  since  $\overline{K_1}(p)/K_1$  is normal and  $\text{Gal}(K_2/K_1)$  is just the factor group of  $\text{Gal}(\overline{K_1}(p)/K_1)$  by the normal subgroup which is generated by the subgroups  $T_p$  (formed with respect to  $\text{Gal}(\overline{K_1}(p)/K_1)$ ) for all  $p \notin S_2$ . Then from well-known general properties of free pro- $p$ -products ([12]) we can easily derive the desired statements. In other words, without loss of generality we assume  $S_2 = \text{set of all primes of } k$ .

By a cohomological criterion of J. Neukirch [12] we need

only show that the restriction map

$$H^i(\overline{K_1}(p)/K_1, \mathbb{Z}/p\mathbb{Z}) \rightarrow \prod_{p \notin S_1} H^i(T_p, \mathbb{Z}/p\mathbb{Z}) \quad (4.6)$$

is injective for  $i = 2$  and surjective for  $i = 1$ . There is nothing to prove for  $i = 2$ , since all cohomology groups in question vanish.

Now we consider the map (4.6) for  $i = 1$  in more detail. The restricted product  $\prod$  is actually the direct sum  $\coprod$ . Furthermore, we have naturally injective maps

$$H^1(T_p, \mathbb{Z}/p\mathbb{Z}) \rightarrow \prod_{\substack{P_1 \\ P_1/p}} H^1(T_{P_2}, \mathbb{Z}/p\mathbb{Z}) \quad (4.7)$$

since each group  $T_p$  is generated by the groups  $T_{P_2}$  (we recall that each  $P_2$  is a fixed prolongation of  $P_1$ ). The local inflation at all primes  $P_1$  in  $K_1$  give rise to homomorphisms

$$H^1(T_{P_2}, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^1(\overline{K_1}_{P_1}/K_1, \mathbb{Z}/p\mathbb{Z}) \quad (4.8)$$

If we take into account the natural isomorphism

$$H^1(\overline{K_1}(p)/K_1) \xrightarrow{\sim} H^1(\overline{k}/K_1, \mathbb{Z}/p\mathbb{Z}) \quad (4.9)$$

we obtain from (4.6), (4.7) and (4.8) the composed homomorphism

$$H^1(\bar{k}/K_1, \mathbb{Z}/p\mathbb{Z}) \rightarrow \coprod_{p \notin S_1} \prod_{\substack{P_1 \\ P_1/p}} H^1(\bar{K}_1, P_1 / K_1, P_1, \mathbb{Z}/p\mathbb{Z}) \quad (4.10)$$

Now it is clear enough that it would suffice to prove the surjectivity of the morphism (4.10). Using the isomorphisms (4.2) and (4.3) we can interpret the map (4.10) by way of the canonical map of limits over  $L$  ( $L/k$  finite). For this reason we consider a part of Tate's long exact sequence ([17], [3]) over a finite field  $L$  ( $L \supset k$ ) contained in  $K_1$ :

$$\begin{aligned} H^1(\bar{k}/L, \mathbb{Z}/p\mathbb{Z}) &\rightarrow \coprod_p \sum_{P/p} H^1(\bar{L}_P/L_P, \mathbb{Z}/p\mathbb{Z}) \\ &\rightarrow H^1(\bar{k}/L, \mu_p)^* \rightarrow H^2(\bar{k}/L, \mathbb{Z}/p\mathbb{Z}) \end{aligned} \quad (4.11)$$

taking inductive limits over  $L$  with regard to the restriction maps and remembering that

$$\lim_{\rightarrow} H^2(\bar{k}/L, \mathbb{Z}/p\mathbb{Z}) = H^2(\bar{k}/K_1, \mathbb{Z}/p\mathbb{Z}) = 0$$

by virtue of  $\text{cd}_p \text{Gal}(k/K_1) \leq 1$  or by theorem 2 a). From the resulting sequence

$$\begin{aligned} H^1(\bar{k}/K_1, \mathbb{Z}/p\mathbb{Z}) &\rightarrow \\ \lim_{\rightarrow} \coprod_{p \in S_1} \sum_{P/p} H^1(\bar{L}_P/L_P, \mathbb{Z}/p\mathbb{Z}) &\times \lim_{\rightarrow} \coprod_{p \notin S_1} \sum_{P/p} H^1(\bar{L}_P/L_P, \mathbb{Z}/p\mathbb{Z}) \\ &\rightarrow \lim_{\rightarrow} H^1(\bar{k}/L, \mu_p)^* \rightarrow 0 \end{aligned} \quad (4.13)$$

it is readily checked that (4.10) is surjective if and only if the map

$$\lim_{\rightarrow} \coprod_{p \in S_1} \sum_{P/p} H^1(\overline{L_P}/L_P, Z/pZ) \rightarrow \lim_{\rightarrow} H^1(\overline{k}/L, \mu_p)^* \quad (4.12)$$

is surjective. By dualizing and using Tate's local duality we get the condition that

$$\lim_{\leftarrow} H^1(\overline{k}/L, \mu_p) \rightarrow \lim_{\leftarrow} \coprod_{p \notin S_1} \sum_{P/p} H^1(\overline{L_P}/L_P, \mu_p) \quad (4.14)$$

must be injective. The inverse limits are taken with respect to the corestriction maps. Denote the kernel of (4.14) by  $C$ . In view of the isomorphism  $H^1(\overline{k}/L, \mu_p) \cong L^\times/L^{\times p}$  an element of  $C$  is a vector  $(\alpha(L) \bmod L^{\times p} | L \subset K_1)$  with  $\alpha(L) \in L^\times$ ,  $\alpha(L) \bmod L^{\times p} = \text{Norm}_{M/L} \alpha(M) \bmod L^{\times p}$  for all  $M$  with  $M \supseteq L$  and  $\alpha(L) \in (L_P^\times)^p$  for all  $P \in S_1(L)$ . As Neukirch [11], §11, remarks, for the  $L$ -coordinate  $\alpha(L)$  the principal ideal  $(\alpha(L))$  is the  $p$ -th power of an ideal  $a(L)$  in  $L$ . Indeed, take a prime  $P$  of  $L$  with  $P \notin S_1(L)$  occurring in the decomposition of  $(\alpha(L))$ . Then there exists in the cyclotomic  $\mathbb{Z}_p$ -extension  $K_0/k$  (resp.  $K_0/k(\sqrt{-1})$  for  $p = 2$ ) a sufficiently large field  $M$  such that in the extension  $ML/L$   $P$  splits into prime factors whose relative degrees are multiples of  $p$ . Now we deduce from the relation

$$\alpha(L) = \text{Norm}_{ML/L} \alpha(ML) \cdot \beta^p, \quad ML \subset K_1$$

that the exponent of  $P$  in  $(\alpha(L))$  is divisible by  $p$ . So we see that  $\alpha(L)$  is contained in  $V_{S_1}(L)$ . The group  $C$  can be identified with the limit

$$\lim_{\leftarrow} V_{S_1}(L)/L^{\times p}$$

It remains to repeat an argument given in the proof of theorem 2 a) and to apply corollary 3.2. Thus we see that  $C = \{1\}$ , i.e., that (4.14) is injective, Q.E.D.

To complete the proof we have to show (1.6) and (1.7). Take a prime  $P_2$  in  $K_2$  dividing some  $p \in S_2 \setminus S_1$ . It follows that  $p \nmid p$  and that  $P_2$  is tamely ramified in  $K_2/K_1$ . But, if  $\delta(K_2, P_2) = \delta(K_1, P_1) = 0$ , all  $p$ -extensions  $M/L$  where  $L$  is a finite subfield of  $K_1$  are unramified at the prime lying under  $P_2$ . Passing to the limit we see that (1.6) is true. Suppose now that  $\delta(K_2, P_2) = \delta(K_1, P_1) = 1$ . To prove (1.7) for arbitrary sets  $S_2$  it suffices to prove it for the maximal  $p$ -extension  $\overline{K_1}(p)/K_1$ . This follows straightforwardly from the decomposition of  $\text{Gal}(\overline{K_1}(p)/K_1)$  into a free pro- $p$ -product. Let  $P_1$  be the prime of  $K_1$  lying under  $P_2$ . For a sufficiently large finite subfield  $L$  of  $K_1$  and the prime  $p$  lying under  $P_1$  we have  $\delta(L_p) = 1$  and in addition  $\sqrt{-1} \in L$  in the case  $p = 2$ .  $P_1$  is unramified in  $K_1/L$  and the localization of  $K_1$  at  $P_1$  contains the maximal unramified

$p$ -extension of  $L_p$ . The maximal  $p$ -extension  $\overline{K}_1(p)/K_1$  contains the maximal  $p$ -extension  $\overline{L}(p)/L$ . To prove (1.7) it suffices to prove that in  $\overline{L}(p)/L$  all inertia groups associated to  $p$  are isomorphic to  $\mathbb{Z}_p$ . This fact can be proved using the existence theorem of Grunwald-Hasse-Wang (s. Neukirch loc. cit.). We prefer to quote here an alternative proof within the framework of  $p$ -extensions. There exists in  $L$  a finite set  $S$  of primes such that  $S \supseteq S_0$ ,  $p \notin S$  and  $V_S(L) = L^{\times p}$ . Put  $S' = S \cup \{p\}$  and consider the  $p$ -extensions  $L_S(p)/L$  and  $L_{S'}(p)/L$ . Let  $T$  be the inertia group in  $\text{Gal}(L_{S'}(p)/L)$  associated to some fixed prolongation of  $p$ . Obviously,  $\text{Gal}(L_S(p)/L)$  is the factor group of  $\text{Gal}(L_{S'}(p)/L)$  by the normal subgroup generated by  $T$ . On the other hand, the well-known formulae for the number of generators of the groups  $\text{Gal}(L_S(p)/L)$  and  $\text{Gal}(L_{S'}(p)/L)$  show that these numbers actually differ by 1 (see [5], prop. 11.8; [15] theorem 1). From this we can conclude that  $T \neq \{1\}$ . We know that  $\text{cd}_p T \leq 2$  in virtue of  $\text{cd}_p \text{Gal}(L_{S'}(p)/L) \leq 2$ .  $T$  is a homomorphic image of  $\mathbb{Z}_p$  and hence the only remaining possibility is  $T \cong \mathbb{Z}_p$ .

The proof of theorem 2 is complete. At the same time we have proved that the morphisms (4.8) are isomorphisms.

§5. Some consequences of theorem 2

Let  $k$  be a finite number field,  $p$  a rational prime. By  $S_0$  we shall denote the set of primes of  $k$  consisting of the archimedean ones and of the divisors of  $p$ .

Corollary 5.1. Let  $q$  be a prime of  $k$  with  $q \nmid p$  and let  $i: \bar{k} \rightarrow \bar{k}_q$  be a fixed injection. Then the image of the maximal  $p$ -extension  $k_{S_0 \cup \{q\}}(p)/k$  unramified outside  $S_0 \cup \{q\}$  under  $i$  is just the maximal  $p$ -extension of  $k_q$ :

$$i(k_{S_0 \cup \{q\}}(p)) = \bar{k}_q(p). \quad (5.1)$$

Proof. If  $N(q) \not\equiv 1 \pmod{p}$  then  $\bar{k}_q(p)$  coincides with the maximal unramified  $p$ -extension of  $k_q$ . In this case we have  $k_{S_0 \cup \{q\}}(p) = k_{S_0}(p) \supseteq K_0$  where  $K_0/k$  (resp.  $K_0/k(\sqrt{-1})$  for  $p = 2$ ) denotes the cyclotomic  $\mathbb{Z}_p$ -extension. Obviously, we have  $i(K_0) = \bar{k}_q(p)$ . If  $N(q) \equiv 1 \pmod{p}$  then the inertia group of  $\bar{k}_q(p)$  is isomorphic to  $\mathbb{Z}_p$ .  $i(K_0)$  is the maximal unramified  $p$ -extension of  $k_q$ , and by theorem 2 b) all the inertia groups in  $\text{Gal}(k_{S_0 \cup \{q\}}(p)/k)$  associated to  $q$  are isomorphic to  $\mathbb{Z}_p$  (in view of  $\delta(k_q) = 1$ ). Hence, (5.1) is proved.



Corollary 5.2. If  $p \neq 2$  and if  $k_{S_0}(p)/k$  coincides with the cyclotomic  $\mathbb{Z}_p$ -extension  $K_0/k$  then for any set  $S$  of primes of  $k$  with  $S \supseteq S_0$  we have

$$\text{Gal}(k_S(p)/k) \cong * T_P \quad (5.2)$$

where  $P$  runs over all primes of  $K_0$  dividing the primes in  $S \setminus S_0$  and where  $T_P$  denotes the inertia group of some (arbitrarily chosen) prolongation of  $P$ . We have  $T_P \cong \mathbb{Z}_p$  or  $\{1\}$  according as  $\delta(K_0, P) = 1$  or  $0$ .

Proof. Obviously, it will be sufficient to prove (5.2) in the case  $S =$  set of all primes of  $k$ ,  $k_S(p) = \bar{k}(p)$ . The proof of theorem 2 b) carries over almost literally to our corollary. But the crucial fact under our assumptions is that the decomposition group of any  $p \notin S_0$  in the extension  $K_0/k$  is of finite index in  $\text{Gal}(K_0/k)$ . Thus over  $p$ ,  $p \notin S_0$ , lies always only a finite number of primes  $P$  in  $K_0$ . Therefore, in the maps (4.7) and (4.10) the symbol  $\prod_P$  can be replaced by the symbol  $\coprod_P$  for the direct sums. This leads immediately to the decomposition (5.2).

The assumptions of corollary 5.2. are fulfilled in the case  $p \neq 2$ ,  $k = \mathbb{Q}$  and give a theorem of Neukirch ([11], theorem 11.3).

Corollary 5.3. Let  $S, T$  be sets of primes of  $k$  with  $T \supseteq S \supseteq S_0$ . Let  $\{\bar{\sigma}_i \mid i \in I\}$  be a minimal system of topological generators of  $G_S = \text{Gal}(k_S(p)/k)$  and  $\{\sigma_i \mid i \in I\}$  be a system of elements of  $G_T = \text{Gal}(k_T(p)/k)$  with  $\sigma_i \bmod \text{Gal}(k_T(p)/k_S(p)) = \bar{\sigma}_i$ . Further, suppose that for each  $p, p \in T \setminus S$ ,  $N(p) \equiv 1 \pmod{p}$  an element  $\tau_p \in G_T^S = \text{Gal}(k_T(p)/k_S(p))$  is given such that  $\tau_p$  generates the inertia group of some prolongation of  $p$ . Then the following assertions hold.

- a) The elements  $\tau_p$  form a system of  $G_T$ -generators of  $G_T^S$  ( $G_T$  acts on  $G_T^S$  by inner automorphisms).
- b) The set  $\{\sigma_i, \tau_p \mid i \in I, p \in T \setminus S, N(p) \equiv 1 \pmod{p}\}$  forms a set of generators of  $G_T$  where the subset  $\{\tau_p\}$  is free.
- c) This set is a minimal one if  $S$  is finite and  $V_S = k^{\times p}$ . Moreover, in this case the elements  $\tau_p$  form a minimal set of  $G_T$ -generators of  $G_T^S$ .

It should be emphasized that the corollaries 5.2 and 5.3 complete the known results about the groups  $G_T$  in terms of generators and relations (in particular cf. [5], 11.4 and 11.5).

Proof. To prove a) we remark only that  $G_T^S$  is just the normal subgroup of  $G_T$  which is generated by the  $\tau_p$ 's. To prove b) by Burnside's basis theorem we must consider the images of the  $\sigma_i$  and the  $\tau_p$  under the epimorphism  $G_T \rightarrow G_T / (G_T^S)^*$  where  $(G_T^S)^*$  denotes the group  $(G_T^S)^p$ .  $[G_T, G_T]$ . Let  $U = (\sigma_i \mid i \in I) \subseteq G_T$  be the closed subgroup generated by the  $\sigma_i$ . Obviously,  $U$  together with  $G_T^S$  generates the whole group  $G_T$ . Let  $(G_T^S)^*$  denote the group  $(G_T^S)^p$ .  $[G_T, G_T^S]$ . The inclusion  $(G_T^S)^* \subseteq (G_T)^*$  induces an epimorphism

$$G_T^S / (G_T^S)^* \rightarrow G_T^S \cdot (G_T)^* / (G_T)^*. \quad (5.3)$$

Now it is easy to see that the group  $G_T^S$  contributes just the elements  $\tau_p$  to a set of generators of  $G_T$ , since by a) the images of the  $\tau_p$ 's certainly span the space  $G_T^S / (G_T^S)^*$ . By virtue of (1.5), the subset  $\{\tau_p\}$  is free. Let us assume now that  $S$  is finite and  $V_S = k^{\times p}$ . To begin with we restrict ourselves to finite sets  $T$ . According to well-known results (see [15], [5]) the number of generators of  $G_S$  resp.  $G_T$  is equal to

$$d(G_S) = [k : \mathbb{Q}] - \delta(k) - r + 1 + \sum_{p \in S} \delta(k_p) \quad (5.4)$$

resp. to

$$d(G_T) = [k : \mathbb{Q}] - \delta(k) - r + 1 + \sum_{p \in T} \delta(k_p) \quad (5.5)$$

( $r$  is the number of archimedean valuations on  $k$ ). In our case the set  $\{\sigma_i, \tau_p\}$  has just the cardinality

$$d(G_S) + \sum_{p \in T \setminus S} \delta(k_p) = d(G_T)$$

and, therefore, is a minimal one. Moreover, the epimorphism (5.3) is an isomorphism now. Hence, the  $\tau_p$ 's constitute a minimal set of  $G_T$ -generators of  $G_T^S$ . Arbitrary sets  $T$  are dealt with by passing to the limit over finite subsets. All assertions of corollary 5.3 are proved.

I would like to thank D. Zagier who corrected the grammar and expression of a part of this note.

#### REFERENCES

1. Brumer A., Galois groups of extensions of algebraic number fields with given ramification. Michigan Math. J. 13 (1966), 33-40.
2. Cassels J.W.S. and Fröhlich A., Algebraic Number Theory. London and New York 1967.
3. Haberland K., Der Tatesche Dualitätssatz aus der Galois-Cohomologie über Zahlkörpern. Dissertation Berlin 1975.
4. Koch H., Fields of class two and Galois cohomology, Durham Symposium.
5. Koch H., Galoissche Theorie der  $p$ -Erweiterungen. Berlin 1970 (Russian translation Moscow 1973).

6. Koch H., Zur Galoisschen Theorie der maximalen  $p$ -Erweiterungen mit vorgegebenen Verzweigungsstellen. Math. Nachr. 61 (1974), 47-50.
7. Kuz'min L.V., Homology of profinite groups, Schur's multiplier and classfield theory. Izv. Ak. nauk SSSR. Ser. mat., 33 (1969), 1220-1254. (Russ.)
8. Kuz'min L.V., The Tate module of an algebraic number field (Russ.). Izv. Ak. nauk SSSR. Ser. mat. 36 : 2 (1972), 267-327.
9. Magnus W., Über diskontinuierliche Gruppen mit einer definierenden Relation (Der Freiheitssatz). J. reine u. angew. Math. 163 (1931), 141-165.
10. Mazur B., Notes on étale cohomology of number fields. Ann. Sci. E. N. S., 4<sup>e</sup> série (6) (1973), 521-553.
11. Neukirch J., Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen. J. reine u. angew. Math., 259 (1973), 1-47.
12. Neukirch J., Freie Produkte pro-endlicher Gruppen und ihre Kohomologie. Archiv der Math., 22 (1971), 337-357.
13. Neumann O., On  $p$ -closed fields of algebraic numbers with restricted ramification (Russ.). Izv. Ak. nauk SSSR. Ser. mat. 39 : 2 (1975), 259-271.
14. Šafarevič I.R., Algebraic number fields (Russ.). Proceed. Intern. Congress Math. Stockholm (1962), 163-176.
15. Šafarevič I.R., Extensions with given ramification points (Russ.). Publ. Math. I.H.E.S. (1964) No. 18, 71-95.
16. Serre J-P., Cohomologie Galoisienne. Lecture Notes Math. No. 5 Berlin-Göttingen-Heidelberg 1964.
17. Tate J., Duality theorems in Galois cohomology over number fields. Proceed. Intern. Congr. Math. Stockholm (1962), 288-295.



# Holomorphy of Quotients of Zeta-Functions

Robert W. van der Waall

## Introduction

Let  $K$  be an algebraic number field (extension field of finite degree of the rational field  $\mathbb{Q}$ ). Consider the Zeta-function

$$\zeta_K(s) = \sum_a (Na)^{-s},$$

defined in the domain  $\operatorname{Re}(s) > 1$ , the summation being extended over all integral ideals of  $K$ . Here  $N$  is the so-called absolute norm, that is  $Na = \prod_{i=1}^r (Np_i)^{e_i}$ , if  $a = p_1^{e_1} \dots p_r^{e_r}$  is the decomposition of  $a$  in prime ideals  $p_i$  of  $K$  and  $Np_i$  is the number of elements in the residue field  $\overline{K}_{p_i}$ .

The zeta-function  $\zeta_K(s)$  converges absolutely and uniformly in the domain  $\operatorname{Re}(s) \geq 1 + \delta$ , any  $\delta > 0$ . It was E. HECKE [5] who found the functional equation for  $\zeta_K(s)$ , and proved that  $\zeta_K(s)$  has an analytic continuation over the whole complex plane, with the sole exception at the point



$s = 1$ , where there is a pole. Notice that  $\zeta_Q(s)$  is just the ordinary Riemann zeta-function.

It is the purpose of this paper to give a short historical survey on the development and advances concerning the following problem, the first investigations on it going back to DEDEKIND ( $\sim 1873$ ) :

Problem: Let  $L$  be a finite extension of  $K$ . Is  $\zeta_L(s)/\zeta_K(s)$  holomorphic in the whole complex plane?

If for a certain choice of  $L$  and  $K$  this problem has an affirmative answer, then we will say:  $P(L/K)$  holds. All the notations and conventions are more or less standard and can be found in [3] and [7]. For background on L-functions see also [15].

I hope I have quoted the most important sources. If some have been forgotten, then I would like to apologize.

The classical way of attacking this problem is by means of group theory, more precisely, by character theory of finite groups. Namely, let  $\Omega \supseteq L$  be a field extension such that  $\Omega/K$  is a galois extension with finite galois group. Let  $\eta$  be the trivial character of  $\text{Gal}(\Omega/L)$ ,  $\eta^G$  the induced

character to  $G = \text{Gal}(\Omega/K)$ , and let  $\lambda$  be the trivial character of  $G$ . In all cases for which  $P(L/K)$  is known to hold, the methods of establishing  $P(L/K)$  are based -either explicitly or implicitly- on the fact that, for those extensions  $L/K$ ,  $\eta^G - \lambda$  is a linear combination of monomial characters  $\lambda_i$ ,  $\lambda_i \neq \lambda$ , with positive rational coefficients  $t_i$  (i.e.  $\eta^G - \lambda = \sum t_i \lambda_i$ ).<sup>\*(Footnote)</sup> Now, if so, then for some specific positive integer  $n$ ,  $(\zeta_L(s)/\zeta_K(s))^n$  equals a product of L-functions of abelian characters. The latter L-functions are integral functions. This is not trivial, and based on investigations of Weber on L-functions for class fields, on the proof of Takagi that all relative abelian fields are class fields, and on Hecke's proof of the functional equation of the so-called Hecke-Dirichlet L-functions (cf. [5]). Then, however, it follows that  $P(L/K)$  holds.

In this paper we consider the two cases of the above method which can occur for the extension  $L/K$ .

---

<sup>\*(Footnote)</sup> Recent work of Langlands has however opened a new approach, (See [15] I for reference).

1) Assume that  $L$  is an extension of  $K$ , not solvable by radicals (over  $K$ ). There are two general cases known (to me), to wit:

1a)  $L/K$  is a galois extension with non-solvable galois group. Then  $P(L/K)$  holds by a character result of Brauer, see §3.

1b)  $L$  is contained in a field  $\Omega$  such that  $\Omega/K$  is a galois extension with a non-solvable galois group  $\text{Gal}(\Omega/K)$  which is a Frobenius group, and such that  $\text{Gal}(\Omega/L)$  is the so-called Frobenius complement. See §4 and also [7] for more details.

2) Assume that  $L$  is an extension of  $K$ , solvable by radicals (over  $K$ ). Let  $\Omega$  be an extension of  $L$  such that  $\text{Gal}(\Omega/K)$  is a finite solvable group. All authors, except those of [8], [10] and [12], deal with solvable galois groups of a specific prescribed nature (In [8] there is a prescribed nature but the word "solvable" is not important there). See §§1,2,3.

However,  $P(L/K)$  holds in fact for any solvable  $\text{Gal}(\Omega/K)$ .

The last result has been found in 1974 and is fully described in [10] and [12].

Although ARTIN [1] was the first to investigate the problem in the version as stated above, i.e. stressing the holomorphy of  $\zeta_L(s)/\zeta_K(s)$ , we will refer to this problem as

DEDEKIND's problem, as a token of homage to him, as initiator of the problem.

# 1. R. Dedekind

In [4], §§6-8, published in 1900, R. DEDEKIND gives the explicit details of the following statement, solved already by him in about 1873:

Statement: Let  $L$  be an extension of the rational field  $Q$  such that  $[L:Q] = 3$ ,  $L = Q(\sqrt[3]{a})$ ,  $a \in Q$ . Then the function  $\zeta_L(s)/\zeta_Q(s)$  equals

$$L(s, \psi, L(\rho)/Q(\rho)) = \prod_{p \nmid f_\psi} (1 - \psi(p)N(p)^{-s})^{-1}. \quad (1)$$

{We have adopted the following notation for this L-function:  $\rho = \exp(2\pi i/3)$ ;  $\psi$  is a proper non-trivial linear character of the corresponding class group; "proper" means "eigentliche" as in HASSE's Zahlbericht;  $p$  runs through the prime ideals of  $Q(\rho)$ , not dividing the ideal  $f_\psi$ , the conductor of  $\psi$ . The notation for this L-function is in agreement with the notion of the so-called second definition of the Artin L-function, see [15], with respect to the cyclic group  $\text{Gal}(L(\rho)/Q(\rho))$  of order 3}.

DEDEKIND does not say anything about the functional equation of  $\zeta_L(s)/\zeta_Q(s)$ , whence also nothing about the holomorphy of it. HECKE [5] found the functional equation for the so-called HECKE-DIRICHLET L-functions, from which it follows that the abelian function  $L(s, \psi, L(\rho)/Q(\rho))$  can be holomorphically extended over the whole complex plane.

## 2. E. Artin

In [1] (1923), E. ARTIN mentions DEDEKIND's paper [4]. He refers to the theorem of TAKAGI [9], that

Every field  $L$ , finite over  $K$ , and such that  $L/K$  is galois with abelian galois group is a class field with respect to  $K$ .

Using this one derives by an argument going back to WEBER [13], that, in the latter situation,

$\zeta_L(s) = \zeta_K(s) \prod_{\chi} L(s, \chi)$ , where  $\chi$  runs through all distinct proper non-principal characters of the corresponding class group. Therefore DEDEKIND's problem has an affirmative answer in this case.

Thus, if in general  $L/K$  is a tower of fields such that

$L = L_1 \supset L_2 \supset \dots \supset L_n = K$  with  $L_i/L_{i+1}$  galois and abelian, then  $P(L/K)$  holds and hence if

$L/K$  is galois such that  $\text{Gal}(L/K)$  is solvable, (2)

then  $P(L/K)$  holds.

ARTIN moreover proved the following two results:

If  $L/K$  is galois and  $\text{Gal}(L/K)$  is isomorphic to the alternating group  $A_5$  on five symbols then  $P(L/K)$  holds. (3)

Let  $L$  be an extension of  $K$  such that  $[L:K] = p^n$ ,  $p$  prime.

Consider  $\Omega \supset L \supset K$  such that  $\Omega$  is galois over  $K$ . Suppose that  $\text{Gal}(\Omega/K) \cong G$  with  $G = \{\text{all maps } f, z \mapsto az + b, a \neq 0, a \in \mathbb{F}_n, z, b \in \mathbb{F}_n\}$ , so  $G$  has order  $p^n(p^n - 1)$  and  $G (= L_p$  in Huppert's notation in [7]) is a so-called linear group. Then  $P(L/K)$  holds. (4)

Notice that we are in DEDEKIND's case when putting  $p = 3$  and  $n = 1$ . Observe that  $G$  is solvable.

The last case done by ARTIN was:

Let  $\Omega \supset L \supset K$  such that  $\Omega$  is galois over  $K$  with

$\text{Gal}(\Omega/K) \cong S_4$ , the symmetric group on four symbols and

let  $[L:K] = 4$ . Then  $P(L/K)$  holds. (5)

For the details of the proofs see ARTIN's original paper [1].

### 3. R. Brauer

It is R. BRAUER who exploited character theory of group representations in a systematic way for our problem. We have the theorem proved in [2] (1947):

Let  $G$  be a finite group and let  $\chi_1, \dots, \chi_k$  be the set of the distinct irreducible complex characters of  $G$ . Let  $g$  be the order of  $G$ . Suppose  $\chi_1$  is the trivial character of  $G$ . Then

$$g \left( \sum_{i=1}^k \chi_i(1) \chi_i - \chi_1 \right) = \sum_j n_j \psi_j^*, \quad n_j \text{ some non-negative integers.}$$

The  $\psi_j^*$  are characters of  $G$  induced by  $\psi_j$  with  $\psi_j$  some linear character, non-trivial for all  $j$ , of some subgroup  $H_j$  of  $G$ . (6)

Therefore if  $L$  is a galois extension of  $K$  such that  $\text{Gal}(L/K) \cong G$ , then by ARTIN's formalism and by (6):

$$[\zeta_L(s)/\zeta_K(s)]^g = \prod_j L(s, \psi_j^*, L/K)^{n_j} = \prod_j L(s, \psi_j, L/L_j)^{n_j},$$

where  $L_j$  is the invariant field of  $H_j$ . Then  $P(L/K)$  holds in this case. (7)

(See here [15]).



Observe that BRAUER's result generalizes the cases (2) and (3) of ARTIN. As Brauer points out his theorem had previously been proved by H. Aramata, [14], in 1933.

#### 4. M. Ishida

M. ISHIDA [8] (1957) deals with the following situation:

Let  $\Omega$  be a finite galois extension over  $K$  such that  $\Omega \supset L \supset K$  with  $\text{Gal}(\Omega/K)$  a so-called "Frobenius group to  $H$ " with  $H = \text{Gal}(\Omega/L)$ . Then  $P(L/K)$  holds. (8)

The finite group  $G$  is called a Frobenius group to the subgroup  $H \neq \{1\}$ , if  $H \cap H^t = \{1\}$  for any  $t \in G - H$ .  $H$  is called the Frobenius complement of  $G$ . The set  $F = G - \bigcup_{g \in G} (H - \{1\})^g$  is in fact a normal subgroup of  $G$ , the so-called Frobenius kernel of  $G$ . See [7] for more properties and details. It is known that a Frobenius group is not necessarily solvable ( $H$  can be non-solvable).

Observe that (8) generalizes ARTIN's case (4). Here too character properties of Frobenius groups are used in order to achieve the result.

5. K. Uchida and R. van der Waall

The second author gives in [11] (1974) the following result:

Let  $\Omega/K$  be a galois extension,  $\Omega \supseteq L \supseteq K$ , and let  $\text{Gal}(\Omega/K)$  be a homomorphic image of a subgroup of some solvable finite doubly transitive group  $R$  such that the quaternion group of order eight is not a homomorphic image of any subgroup of  $R$ . Then  $P(L/K)$  holds. (9)

The proof uses HUPPERT's classification of solvable doubly transitive groups [6]. It turns out that our  $\text{Gal}(\Omega/K)$  is monomial and then it can be proved easily that  $P(L/K)$  holds. See [11] for further details.

In 1975 both authors ([10] and [12]) proved independently of each other the

Theorem: Let  $\Omega/K$  be a finite galois extension and let  $L$  be an intermediate field. Suppose that  $\text{Gal}(\Omega/K)$  is solvable. Then  $P(L/K)$  holds. (10)

This generalizes the above results (1), (2), (4), (5)

and (9).

The proof is based on the proposition (cf. [10], [12]).

Proposition Let  $L$  be a finite extension of  $K$ , and suppose that  $\Omega$  is a galois extension of  $K$ , containing  $L$ , such that  $G = \text{Gal}(\Omega/K)$  is a finite solvable group. Furthermore assume that  $H = \text{Gal}(\Omega/L)$  is a maximal subgroup of  $G$  and assume that  $G = HA$ ,  $A$  some normal abelian subgroup of  $G$  with  $H \cap A = \{1\}$ . Let  $\psi$  be the trivial character of  $H$ .

Then

$$\psi^G - \rho = \sum_i n_i \rho_i, \quad ,$$

where the  $\rho_i$  are non-trivial monomial irreducible characters of  $G$ , and where the  $n_i$  are positive rational integers.

$\psi^G$  is defined to be the induced character of  $\psi$  to  $G$ ;  $\rho$  is the trivial character of  $G$ .

It follows from the proposition and using Artin's formalism together with the known properties of the  $L$ -function  $L(s, \rho_i, \Omega/K)$  (it is here an abelian  $L$ -function as  $\rho_i$  is monomial, and thus holomorphic as  $\rho_i$  is not the trivial character) that  $P(L/K)$  holds.

All cases mentioned in this paper, where solvable

groups are involved, depend on field towers where the proposition is valid in every layer.

## 6. Epilogue

Let  $\Omega$  be a galois extension of the algebraic number field  $K$  such that  $\text{Gal}(\Omega/K)$  is isomorphic to  $A_5$ . Then there exists a field  $L$  with  $\Omega \supset L \supset K$  and  $[L:K] = 5$ . It turns out that  $\zeta_L(s)/\zeta_K(s) = L(s, \chi_4, \Omega/K)$ , where  $L(s, \chi_4, \Omega/K)$  is the Artin L-function belonging to the irreducible complex character  $\chi_4$  of  $A_5$  of degree 4.  $\chi_4$  is primitive, i.e., not induced by any irreducible character of some subgroup of  $A_5$ . By a well known result of Brauer (or by a direct trivial observation),  $L(s, \chi_4, \Omega/K)$  is meromorphic. Our tools however do not allow us to decide whether this function is holomorphic or not.

For the sake of completeness we mention that an affirmative answer to the so-called Artin conjecture about Artin L-functions would give an affirmative answer to our problem.

## REFERENCES

1. E. Artin, Ueber die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann., 89 (1923), 147-156.

2. R. Brauer, On the Zeta-function of algebraic number fields, Am. J. of Math. 69 (1947), 243-250,  
Am. J. of Math. 72 (1950), 739-746.
3. J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory, Acad. Press, London, 1967.
4. R. Dedekind, Ueber die Anzahl der Idealklassen der reinen kubischen Zahlkörpern, Journ. f.d. reine u. ang. Math., 121 (1900), 40-123.
5. E. Hecke, Mathematische Werke, Vandenhoeck and Ruprecht, Göttingen, 1959. (Papers 7, 9 and 12).
6. B. Huppert, Zweifach transitive auflösbare Permutationsgruppen, Math. Zeitschrift, 68 (1957), 126-150.
7. B. Huppert, Endliche Gruppen I, Springer Verlag, Berlin-Heidelberg, 1967.
8. M. Ishida, On the Divisibility of Dedekind's Zeta-Functions, Proc. Imp. Ac. Japan, 33, No 6 (1957), 293-297.
9. T. Takagi, Ueber eine Theorie des relativ-Abel'schen Zahlkörpers, J. of the Coll. Sci. imp. Univ. Tokyo, 41, Nr.9 (1920), 1-133.
10. K. Uchida, On Artin L-functions, Tôhoku Math. Journ. 27 (1975), 75-81.
11. R.W. van der Waall, A remark on the zeta-function of an algebraic number field, J.f.d.reine u.ang. Math., 266 (1974), 159-162.
12. R.W. van der Waall, On a conjecture of Dedekind on zeta-functions, Proc. Kon. Ned. Akad.v.Wet. Series A, 78 (1975), 83-86 = Indagationes Mathematicae, 37 (1975), 83-86.
13. H. Weber, Lehrbuch der Algebra III, Braunschweig, 1908, 2<sup>d</sup>-edition, §163 etc.

14. H. Aramata, Proc. Imp. Acad. Tokyo, 7 (1931), 334-336  
and 9 (1933), 31-34.
15. J. Martinet, Character theory and Artin L-functions,  
Durham Symposium.

$$\mathrm{GL}_n$$

W. Casselman

Serre has discussed the correspondence between two-dimensional representations of  $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  of odd determinant and primitive modular forms of weight one, and Tate has talked about how to interpret this in terms of representations of  $\mathrm{GL}_2$ . I want to put all this in a larger context and explain what relationship one expects in general, according to conjectures of Langlands, between representations of Galois groups and of  $\mathrm{GL}_n$ .

If  $k$  is a local field, then local class field theory asserts that there is a natural isomorphism between the maximal abelian quotient of  $W_k$ , the Weil group of  $k$ , and the multiplicative group  $k^\times$  hence also a natural bijection between the set of complex-valued characters of  $W_k$  and those of  $k^\times$ . The local version of Langlands' conjectures is that there is a relationship between continuous,  $n$ -dimensional, complex representations of  $W_k$  and irreducible, admissible



representations of  $GL_n(k)$ . When  $k$  is  $\mathbb{R}$  or  $\mathbb{C}$ , Langlands [19] has in fact defined a bijective correspondence between the two sets which is almost certainly the correct one, and in §1 I shall describe this. The case of non-archimedean  $k$  will be dealt with in §2; the situation is not nearly as satisfactory, but I shall attempt to show what problems have been solved, and what remain. I shall treat global fields in a much more cursory manner in §3, and finally in §4 I shall illustrate a few points by looking at  $GL_2(\mathbb{Q})$  in detail.

This is hardly a survey of the links between arithmetic and representation theory. I have tried merely to show to some extent what some very general conjectures amount to when the group at hand is  $GL_n$ , which is in most ways the simplest of cases. Borel's Séminaire Bourbaki talk last summer [2] is much more comprehensive, although the role of general problems in representation theory is not emphasized. Also, I have concentrated on the local fields  $\mathbb{R}$  and  $\mathbb{C}$  because although the representation theory in this case is older and more developed, it is less clear how much of the subject will prove to be important in arithmetical applications. The answer at this point would seem to be

that a great deal of it is.

A remark about eccentricity in terminology: a character is any continuous homomorphism into  $\mathbb{C}^\times$ , and it is said to be unitary if its image is contained in the unit circle.

## §1. Archimedean fields

Throughout this section,  $k$  will be  $\mathbb{R}$  or  $\mathbb{C}$ .

1.1. The Weil group  $W_{\mathbb{C}}$  is just  $\mathbb{C}^\times$ , while  $W_{\mathbb{R}}$  is the group which corresponds to the extension representing the non-trivial element in  $H^2(\text{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times)$ . Thus it fits into an exact sequence

$$1 \rightarrow \mathbb{C} \rightarrow W_{\mathbb{R}} \rightarrow \text{Gal}(\mathbb{C}/\mathbb{R}) \rightarrow 1.$$

Let  $\tau$  be the conjugation in  $\text{Gal}(\mathbb{C}/\mathbb{R})$ . There exists an element  $F$  in  $W_{\mathbb{R}}$  whose image in  $\text{Gal}(\mathbb{C}/\mathbb{R})$  is such that  $F^2 = -1$  and  $FzF^{-1} = z^\tau$  for all  $z$  in  $\mathbb{C}$ . The norm homomorphism  $\nu$  from  $W_k$  to  $k^\times$  is the identity if  $k = \mathbb{C}$ , while if  $k = \mathbb{R}$  it is characterized by the properties that  $\nu(x) = xx^\tau = \|x\|$  for  $x$  in  $\mathbb{C}$  and  $\nu(F) = -1$ .

Every character of  $W_k$  is of the form  $\chi \cdot \nu$  for some unique character  $\chi$  of  $k^\times$ . I often call it  $\chi$  again.

If  $\chi$  is a character of  $W_{\mathbb{C}}$ , the induced representation

$\text{Ind}(\chi|_{W_{\mathbb{C}}}, W_{\mathbb{R}})$  is two-dimensional. If  $\chi$  is unitary then it is also unitary; in general there will exist a positive real character  $\rho$  of  $W_{\mathbb{R}}$  such that the restriction of  $\chi\rho^{-1}$  to  $W_{\mathbb{C}}$  is unitary, so that  $\text{Ind}(\chi) = \text{Ind}(\chi\rho^{-1}) \oplus \rho$  is at least semi-simple.

1.1.1. Proposition. (a) If  $\chi = \chi^{\tau}$ , then there exists a character  $\rho$  of  $W_{\mathbb{R}}$  whose restriction to  $W_{\mathbb{C}}$  is  $\chi$ , and  $\text{Ind}(\chi)$  is the direct sum of  $\rho$  and  $\rho \cdot \text{sgn}$ ;

(b) If  $\chi \neq \chi^{\tau}$ , then  $\text{Ind}(\chi)$  is irreducible;

(c)  $\text{Ind}(\chi_1) \cong \text{Ind}(\chi_2)$  if and only if  $\chi_1 = \chi_2$  or  $\chi_2^{\tau}$ ;

(d) Any continuous, irreducible, finite-dimensional representation of  $W_k$  is either a character or isomorphic to some  $\text{Ind}(\chi)$  with  $\chi \neq \chi^{\tau}$ .

This is of course well known. For a proof: By Frobenius reciprocity,

$$\text{Hom}_{W_{\mathbb{R}}}(\text{Ind}(\chi_1), \text{Ind}(\chi_2)) \cong \text{Hom}_{W_{\mathbb{C}}}(\text{Ind}(\chi_1), \chi_2) .$$

Since  $W_{\mathbb{R}} = W_{\mathbb{C}} \cup FW_{\mathbb{C}}$ , the restriction of  $\text{Ind}(\chi)$  to  $W_{\mathbb{C}}$  is  $\chi \oplus \chi^{\tau}$ . Since  $\text{Ind}(\chi)$  is semi-simple, this proves (a), (b), and (c). If  $\sigma$  is any continuous, irreducible finite-dimensional representation of  $W_{\mathbb{R}}$ , its restriction to  $W_{\mathbb{C}}$

must have an irreducible quotient. Apply Frobenius reciprocity to prove (d).

As a final point, I remark that if  $\sigma$  is any continuous, irreducible, finite-dimensional representation of  $W_k$ , then there exists a unique positive real-valued character which I call  $|\sigma|$  such that  $\sigma \otimes |\sigma|^{-1}$  is unitary.

1.2. For the moment, let  $G$  be the group of  $\mathbb{R}$ -valued points on an arbitrary reductive algebraic group defined over  $\mathbb{R}$ . (By restriction of the ground field, this includes the possibility of groups over  $\mathbb{C}$ .) Let  $K$  be a maximal compact subgroup of  $G$ ,  $Z_G$  the centre of  $G$ . Let  $\mathfrak{g}$  be the complexified Lie algebra of  $G$ ,  $\mathfrak{k}$  that of  $K$ .

I define an admissible representation of  $\mathfrak{g}$  and  $K$  or (by an abuse of language) of  $G$  to be a complex representation  $(\pi, V)$  of  $\mathfrak{g}$  and  $K$  simultaneously on the same space  $V$  such that (1) the restriction to  $K$  is an algebraic direct sum of finite-dimensional, continuous, irreducible representations, each isomorphism class occurring with finite multiplicity; (2) the representations of  $K$  and of  $\mathfrak{g}$  are compatible, in that the two representations of  $\mathfrak{k}$  one

obtains - as Lie algebra of  $K$  and as subalgebra of  $\mathfrak{g}$  - are the same, and for any  $X \in \mathfrak{g}$  and  $k \in K$  one has  $\pi(k) \pi(X) \pi(k)^{-1} = \pi(\text{Ad}(k)X)$ . This definition depends on the choice of  $K$ , but since all maximal subgroups of  $G$  are conjugate the two categories one obtains from two choices are equivalent.

If  $(\pi, V)$  is admissible, then its contragredient  $(\tilde{\pi}, \tilde{V})$  is the contragredient representation of  $\mathfrak{g}$  and  $K$  on the  $K$ -finite vectors in the algebraic dual of  $V$  - i.e., those vectors contained in some finite-dimensional  $K$ -stable subspace. It is again admissible.

If  $\pi$  were a representation of  $G$ , then one could define for every  $v \in V$ ,  $\tilde{v} \in \tilde{V}$  the function  $c_{v, \tilde{v}}(g) = \langle \pi(g)v, \tilde{v} \rangle$  on  $G$ , called the matrix coefficient associated to the pair. For a fixed  $\tilde{v} \in \tilde{V}$  the map  $v \mapsto c_{v, \tilde{v}}$  would be a  $G$ -morphism from  $V$  to the space of complex functions on  $G$  (with  $G$  acting on the latter by the right regular representation  $R$ ). Even without the action of  $G$ , however, one has:

1.2.1. Theorem If  $(\pi, V)$  is admissible then there exists a unique bilinear map from  $V \times \tilde{V}$  to the space of complex-valued functions on  $G$ ,  $(v, \tilde{v}) \mapsto c_{v, \tilde{v}}$ , such that

for all  $v \in V$ ,  $\tilde{v} \in \tilde{V}$ ,  $X \in \mathfrak{g}$ ,  $k \in K$  :

$$(a) \quad c_{\pi(X)v, \tilde{v}} = R(X)c_{v, \tilde{v}} ;$$

$$(b) \quad c_{\pi(k)v, \tilde{v}}(g) = c_{v, \tilde{v}}(gk)$$

$$c_{v, \pi(k)\tilde{v}}(g) = c_{v, \tilde{v}}(k^{-1}g);$$

$$(c) \quad c_{v, \tilde{v}}(1) = \langle v, \tilde{v} \rangle .$$

If  $\pi$  is irreducible, this is due to Harish-Chandra; it is a consequence of his result that every irreducible admissible representation is a composition factor of some principal series representation ([27] 5.5.1.5). For arbitrary  $\pi$  it seems to be new. It follows from a complicated analysis of the differential equations on the group which the matrix coefficients must satisfy (see [7]).

It is because of this theorem that the definition of admissibility given above is equivalent to that of Jacquet and Langlands. It allows one to define a representation of their Hecke algebra on  $V$ , and hence the character of an admissible representation (which is a linear functional on the algebra). As follows from §7 of [16], a semi-simple representation is determined by its character.



The point of admissible representations is that while they are only representations of  $\mathfrak{g}$ , they are intimately related to those of  $G$  itself. Going from representations of  $G$  to those of  $\mathfrak{g}$  is classical (this is well explained in [1]), and the converse is a consequence of Theorem 1.2.1:

1.2.2. Corollary Any admissible representation of  $\mathfrak{g}$  and  $K$  is isomorphic to the  $\mathfrak{g}$ -stable subspace of  $K$ -finite vectors in some differentiable representation of  $G$ .

This extension is by no means unique, but Jacquet has pointed out that there is a minimal one.

If  $\pi$  is admissible and irreducible, then because of the assumption on finite  $K$ -multiplicity any operator on  $V$  which commutes with  $\mathfrak{g}$  is scalar. Thus there exists a homomorphism  $\theta_\pi : Z(\mathfrak{g}) \rightarrow \mathbb{C}$  according to which  $Z(\mathfrak{g})$ , the centre of the enveloping algebra  $U(\mathfrak{g})$ , acts on  $V$ , called the infinitesimal character of  $\pi$ . By 1.1.2 there also exists a character  $\zeta_\pi : Z_G \rightarrow \mathbb{C}^\times$  according to which  $Z_G$  acts, called the central character of  $\pi$ . The maximal split torus in the centre of  $G$  is isogenous to the maximal split torus in the maximal abelian quotient of  $G$ , and hence for every



$\pi$  there exists a unique positive real character  $|\pi|$  of  $G$  such that the central character of  $\pi \otimes |\pi|^{-1}$  is unitary.

Let  $P$  be a parabolic subgroup of  $G$  with Levi decomposition  $P = MN$ ,  $\delta = \delta_P$  the modulus character of  $M$  with respect to the Lie algebra  $\mathfrak{n}$  of  $N$ :  $m \mapsto |\det \text{Ad}_{\mathfrak{n}}(m)|$ . If  $(\sigma, U)$  is a continuous finite-dimensional representation of  $M$ , then the representation  $\text{Ind}(\sigma|P, G)$  of  $g$  and  $K$  induced by  $\sigma$  is the right regular representation on the space of all  $K$ -finite  $f : G \rightarrow U$  such that  $f(nmg) = \sigma \delta^{\frac{1}{2}}(m)f(g)$  for all  $n \in N$ ,  $m \in M$ ,  $g \in G$ . This is called a principal series representation of  $G$ . If  $\sigma$  is any admissible representation of  $M$  then one can define  $\text{Ind}(\sigma)$  similarly by first embedding  $\sigma$  into a differentiable representation of  $M$ , applying 1.1.2. One can see easily that  $\text{Ind}(\sigma)$  is admissible, because of the Iwasawa decomposition  $G = PK$ . If  $\sigma$  is of finite length, so is  $\text{Ind}(\sigma)$ . (This is a non-trivial fact which follows from very general theorems of Harish-Chandra. In the case when  $\sigma$  is finite-dimensional and  $P$  is minimal, a more elementary proof can be put together along the lines in [21], however, and the case of arbitrary  $\sigma$  can be reduced to this one.)

The admissible representation  $(\pi, V)$  is called unitary if there exists on  $V$  a positive definite Hermitian inner

product with respect to which the operators in  $\mathfrak{g}$  are skew. Any unitary representation is semi-simple. If  $\sigma$  is unitary so is  $\text{Ind}(\sigma)$ , and consequently it is a direct sum of a finite number of irreducible constituents.

An irreducible admissible  $\pi$  is called square-integrable if  $\zeta_\pi$  is unitary and the matrix coefficients are square-integrable on  $G/Z_G$ . For any fixed  $v_0 \neq 0$  the inner product

$$\langle u, v \rangle = \int_{G/Z_G} c_{u, v_0}(g) \overline{c_{v, v_0}(g)} dg$$

shows  $\pi$  to be unitary in this case. The representation  $\pi$  is called essentially square-integrable if  $\pi \otimes |\pi|^{-1}$  is square-integrable.

An irreducible representation  $\pi$  is called tempered if it is a constituent of some  $\text{Ind}(\sigma)$  with  $\sigma$  square-integrable, and essentially tempered if  $\pi \otimes |\pi|^{-1}$  is tempered. Since  $\text{Ind}(\sigma \otimes \chi) \cong \text{Ind}(\sigma) \otimes \chi$  whenever  $\chi$  is a character of  $G$ , any essentially tempered representation is also a summand of some  $\text{Ind}(\sigma)$ .

Two parabolic subgroups  $P_1$  and  $P_2$  are called associate if there exists  $g \in G$  such that  $gM_1g^{-1} = M_2$ . There is a close relationship between representations induced from associate parabolics:

1.2.3. Proposition Let  $P_1$  and  $P_2$  be two parabolic subgroups,  $\sigma_1$  and  $\sigma_2$  admissible square-integrable representations of  $M_1$  and  $M_2$ . Then  $\text{Ind}(\sigma_1 \mid P_1, G) \cong \text{Ind}(\sigma_2 \mid P_2, G)$  if and only if there exists  $g \in G$  such that  $gM_1g^{-1} = M_2$  and  $\sigma_2 \cong \sigma_1^g$ .

It is actually true that the condition is necessary and sufficient in order for the two to have common constituents, but this is more than I shall need later. The proposition is most easily proved by comparing characters, for which an explicit formula is not hard to obtain ([27] 5.5.3.1).

Fix a minimal parabolic subgroup  $P_\phi$  of  $G$ , a maximal split torus  $A_\phi$  in  $P_\phi$ , and a set of associated simple positive roots  $\Delta$ . For every subset  $\Theta \subseteq \Delta$ , let  $P_\Theta$  be the corresponding standard parabolic with Levi decomposition  $M_\Theta N_\Theta$ , and let  $A_\Theta$  be the maximal split torus in the centre of  $M_\Theta$ . If  $P$  is any parabolic, then it is conjugate to a unique standard parabolic; let  $M, N, A$  be the corresponding subgroups of  $P$ . Associated to each  $\alpha \in \Delta$  is a sort of co-root  $\hat{\alpha} : \mathbb{R}^\times \rightarrow A_\phi$ , whose image is contained in the derived group of  $M_{\Delta - \{\alpha\}}$  and such that  $|\alpha(\hat{\alpha}(x))| < 1$  for  $x \in \mathbb{R}^\times$ ,  $|x| < 1$  (refer to the next section for the example

$$G = GL_n).$$

For any parabolic  $P$  let  $D(P)$  be the set of all positive real characters of  $M$ . Such a character is determined by its restriction to  $A$ , and one may therefore identify  $D(P)$  with the group of positive real characters of  $A$ . If  $P_1 \subseteq P_2$  one has a canonical embedding of  $D(P_2)$  into  $D(P_1)$ . Each  $D(P_\theta)$  may therefore be considered as a subspace of  $D(P_\phi)$ , and to be precise it is the subspace of all  $\chi$  such that  $\chi(\alpha^\wedge(x)) = 1$  for all  $\alpha \in \theta$ ,  $x \in \mathbb{R}^\times$ . Define  $D^+(P_\theta)$  to be the cone in  $D(P_\theta)$  of all  $\chi$  such that  $\chi(\alpha^\wedge(x)) < 1$  for all  $\alpha \in \Delta - \theta$ ,  $x < 1$ . If  $P_1 \subseteq P_2$  then  $D^+(P_2)$  lies in the closure of  $D^+(P_1)$  (with respect to their embeddings into  $D(P_\phi)$ ), and the union of all the  $D^+(P_\theta)$  form the closure of  $D^+(P_\phi)$ , a fundamental chamber in  $D(P_\phi)$  for the Weyl group.

If  $P$  is a standard parabolic,  $P^-$  its opposite, and  $\sigma$  an essentially tempered admissible representation of  $M$  with  $|\sigma| \in D^+(P)$ , then for all  $g \in G$  and  $f \in \text{Ind}(\sigma | P, G)$  the integral

$$T_\sigma(f)(g) = \int_N^- f(ng) \, dn$$

converges, and the map  $f \mapsto T_\sigma(f)$  is a  $G$ -morphism from  $\text{Ind}(\sigma | P, G)$  to  $\text{Ind}(\sigma | P^-, G)$ . (See §3 of [19].)

1.2.4. Theorem If  $\sigma$  is essentially tempered with  $|\sigma| \in D^+(P)$ , then the image of  $\text{Ind}(\sigma \mid P, G)$  with respect to  $T_\sigma$  is irreducible.

Call it  $\text{Ind}^+(\sigma \mid P, G)$ .

1.2.5. Theorem If  $(\pi, V)$  is any irreducible admissible representation of  $G$ , then there exists a unique  $P$  and  $\sigma$  with  $\sigma$  essentially tempered and  $|\sigma| \in D^+(P)$  such that  $\pi \cong \text{Ind}^+(\sigma \mid P, G)$ .

Both these results are due to Langlands (§§3 and 4 of [19]). If  $\pi$  is essentially tempered, for example, then  $P$  is just  $G$ . For generic  $\sigma$  the representation  $\text{Ind}(\sigma)$  is irreducible so that  $\text{Ind}^+(\sigma)$  is the whole of  $\text{Ind}(\sigma)$ . Langlands' proof says nothing about when this is so, but it is not difficult to see, for example, that when  $P$  is minimal one obtains all the irreducible finite-dimensional representations among the  $\text{Ind}^+(\sigma)$ .

As we shall see in the next section in more detail, this reduces the classification of irreducible admissibles, at least for a number of purposes, to these problems:

(1) classifying the square-integrable representations;

(2) determining the components of  $\text{Ind}(\sigma)$  when  $\sigma$  is square-integrable; (3) describing the image of  $\text{Ind}(\sigma)$  under  $T_\sigma$ . Harish-Chandra has solved (1) completely (this is incorporated into Langlands' scheme in §§1 and 2 of [19]) - we shall only need the weak result that  $G$  has no square-integrable representations unless the derived group of  $G$  contains a compact maximal torus. Solving (2) is at the moment an active business (and pursuing most actively is Knapp). Progress on (3) has been poor, except for rather special  $\sigma$ .

1.3. Now let  $G$  be  $\text{GL}_n(\mathbb{R})$  or  $\text{GL}_n(\mathbb{C})$ . In the first case  $K$  may be chosen to be  $O(n)$  and in the second  $U(n)$ . The group  $Z_G$  comprises the scalar matrices and is isomorphic to the multiplicative group of the field. By means of the determinant homomorphism, any character of the multiplicative group gives one of  $G$  as well.

As a minimal parabolic subgroup in either group one may choose the Borel subgroup of upper triangular matrices:

$\{x_{ij} = 0 \text{ for } i > j\}$ . The group  $M_\phi$  may be chosen to be the subgroup of diagonal matrices, isomorphic to the direct product of  $n$  copies of  $k^\times$  and coordinatized by the diagonal



entries:  $x_i = x_{ii}$ . In either case the group  $A_\phi$  is the subgroup of real diagonal matrices. The roots in  $\Delta$  are the characters  $x_i/x_{i+1}$ , parametrized by  $i < n$ . For each such  $i$  the associated co-root takes  $x \in \mathbb{R}^\times$  to the matrix with  $x_j = 1$  ( $j \neq i$  or  $i+1$ ),  $x_i = x$ ,  $x_{i+1} = x^{-1}$ .

The standard parabolic subgroups are best parametrized by ordered partitions  $(n_1, \dots, n_m)$  of  $n$  (so that  $n = n_1 + \dots + n_m$ ). To one of these corresponds the group  $P_\theta$  with  $\theta$  such that  $\Delta - \theta = \{n_1, n_1 + n_2, \dots\}$ . The group  $P_\theta$  is  $\{x_{ij} = 0 \text{ when for some } \ell \text{ one has } i > n_1 + \dots + n_\ell, j < n_1 + \dots + n_\ell + 1\}$ , and  $M_\theta$  is isomorphic to the direct product of the  $GL_{n_i}$ . Representations of  $M_\theta$  correspond to ordered sets  $(\sigma_1, \dots, \sigma_m)$  with  $\sigma_i$  a representation of  $GL_{n_i}$ .

Similarly,  $D(P_\phi)$  may be identified with ordered sets of positive real characters  $(\chi_1, \dots, \chi_n)$ . Define  $\chi > \rho$  to mean that  $\chi(x) < \rho(x)$  whenever  $|x| < 1$ . Then  $D^+(P_\phi)$  is the set of such  $n$ -tuples with  $\chi_1 > \chi_2 > \dots > \chi_n$ . The Weyl group here is  $S_n$ , and the fact that the closure of  $D^+(P_\phi)$  is a chamber for it only means that every  $n$ -tuple of distinct  $\chi_i$  may be reordered uniquely so as to satisfy this condition.

Only when  $n = 1$  or  $2$  and  $k = \mathbb{R}$  does the derived group



of  $G$  (which is  $SL_n$ ) contain a compact maximal torus, so that only in these cases does  $G$  have a square-integrable representation. Any tempered representation of  $G$ , therefore - applying this result to the reductive components of parabolics - must be a constituent of some  $\text{Ind}(\sigma | P, G)$  where the reductive component of  $P$  is a product of copies of  $\mathbb{C}^\times$  ( $k = \mathbb{C}$ ) or  $\mathbb{R}^\times$  and  $GL_2(\mathbb{R})$  ( $k = \mathbb{R}$ ).

The representation theory of  $GL_n$  is much simpler than that of other groups because of:

1.3.1. Theorem If  $\sigma$  is an irreducible admissible square-integrable representation of  $M$ , then  $\text{Ind}(\sigma | P, G)$  is irreducible.

When  $k = \mathbb{C}$  this must be a very old result (although I am not sure to whom it is due), and a nice treatment is given in [11] (where arbitrary complex groups are treated). Special cases when  $k = \mathbb{R}$  are also old, but the general result is, I believe, due to Jacquet and Shalika (unpublished).

This answers question (2) at the end of the previous section for  $G = GL_n$ . It may be restated:

1.3.2. Corollary Let  $(n_1, \dots, n_m)$  be given with  $n_1 + \dots + n_m = n$ . Suppose that for each  $i$  the representation  $\sigma_i$  of  $GL_{n_i}$  is essentially square-integrable, and that  $|\sigma_1| = |\sigma_2| = \dots = |\sigma_m|$ . If  $\sigma = (\sigma_1, \dots, \sigma_m)$  then  $\text{Ind}(\sigma)$  is irreducible.

Note that for  $GL_n$ ,  $|\pi|$  may be considered as a character of  $k^\times$ .

In this terminology, Proposition 1.2.3 becomes:

1.3.3. Proposition Let  $P$  and  $P'$  be two parabolics,  $\sigma$  and  $\sigma'$  essentially square-integrable representations of  $M$  and  $M'$ , with all  $|\sigma_i|$  equal and all  $|\sigma_i'|$  equal. Then  $\text{Ind}(\sigma)$  and  $\text{Ind}(\sigma')$  are isomorphic if and only if the  $\sigma_i$  are a permutation of the  $\sigma_i'$ .

Another translation (of 1.2.4):

1.3.4. Theorem If  $\sigma = (\sigma_1, \dots, \sigma_m)$  with  $|\sigma_1| > \dots > |\sigma_m|$  then the image of  $\text{Ind}(\sigma)$  with respect to  $T_\sigma$  is irreducible.

If one is given  $\sigma$  with  $|\sigma_1| \geq \dots \geq |\sigma_m|$  then one may group the  $\sigma_i$  into blocks of equal magnitude and apply

1.3.3 and 1.3.4 together to induce in steps and determine a certain representation which I still call  $\text{Ind}^+(\sigma)$ , a quotient of  $\text{Ind}(\sigma)$ . Translating 1.2.5 and applying 1.3.3:

1.3.5. Theorem Every admissible representation of  $\text{GL}_n$  is an  $\text{Ind}^+(\sigma)$  for some  $\sigma = (\sigma_1, \dots, \sigma_m)$  with  $|\sigma_1| \geq \dots \geq |\sigma_m|$ . If  $\sigma$  and  $\sigma'$  both satisfy this condition then  $\text{Ind}^+(\sigma)$  and  $\text{Ind}^+(\sigma')$  are isomorphic if and only if  $\sigma$  is a permutation of  $\sigma'$ .

1.4. Recall that there exists a natural identification of a character of  $W_k$  with one of  $k^\times$ . It is shown in [16], among other places, that there also exists a natural bijection between the set of continuous, irreducible, two-dimensional representations of  $W_{\mathbb{R}}$  and that of irreducible, essentially square-integrable, admissible representations of  $\text{GL}_2(\mathbb{R})$ . To each irreducible, continuous representation  $\rho$  of  $W_k$  of dimension  $n$ , therefore, one may associate a certain irreducible, essentially square-integrable, admissible representation of  $\text{GL}_n(k)$ . Call it  $\pi(\rho)$ .

If  $\rho$  is any semi-simple representation of  $W_k$ , say of dimension  $n$ , it will be a direct sum of irreducibles

$\rho_i$  ( $i \leq m$ ), say of dimension  $n_i$ . Each  $\rho_i$  gives rise to a representation  $\pi(\rho_i)$  of  $GL_{n_i}$ , and their direct product  $\sigma$  will be a representation of the reductive component of the parabolic in  $GL_n$  determined by the partition  $n = n_1 + \dots + n_m$ . One may arrange the  $\rho_i$  in any order, and in particular one may choose them so that  $|\rho_1| \geq \dots \geq |\rho_m|$ . Define  $\pi(\rho)$  then to be the representation I call  $\text{Ind}^+(\sigma)$  in §1.3. This is well-defined because any rearrangement of the  $\rho_i$  subject to the given condition gives an isomorphic representation. From Theorem 1.3.5:

**1.4.1. Theorem** The map  $\rho \mapsto \pi(\rho)$  is a bijective correspondence between the set of continuous  $n$ -dimensional semi-simple representations of  $W_k$  and the set of irreducible admissible representations of  $GL_n(k)$ .

Incidentally, it was in order to establish such a correspondence, not only for  $GL_n$  but for other groups as well, that Langlands was motivated to prove Theorems 1.2.4 and 1.2.5. I should say that for other groups the classification and the correspondence are not so simple - first of all because it is not just representations of  $W_k$  but homomorphisms into a certain dual group which play a role,

and second because the analogue of 1.3.1 is false more generally. The correspondence is at best not bijective but one-many.

A strong form of Langlands' conjecture asserts that the L- and  $\varepsilon$ -factors of  $\rho$  and  $\pi(\rho)$  must agree; that for a character  $\chi$  of  $k$ ,  $\pi(\rho \otimes \chi) = \pi(\rho) \otimes \chi$ ; and that  $\zeta_{\pi(\rho)} = \pi(\det \rho)$ . The second and third points are easy to verify, but the first is non-trivial and has not been verified for arbitrary  $\rho$ . For  $GL_2$  this is done in [16], and when  $\text{Ind}^+(\sigma) = \text{Ind}(\sigma)$  follows from the main archimedean results in [15].

## §2. Non-archimedean fields.

In this section, let  $k$  be a non-archimedean field,  $\mathcal{O}$  its ring of integers,  $\mathfrak{p}$  its prime ideal,  $q$  the order of its residue field.

A number of definitions in this section are exact analogues of those for archimedean fields, and I won't repeat them (for example: matrix coefficient, square-integrable representation,  $D(P) \dots$ ).

2.1. Let  $G$  for the moment be the group of  $k$ -rational

points on any reductive algebraic group defined over  $k$ . An admissible representation  $(\pi, V)$  of  $G$  is one such that if  $K$  is any fixed compact open subgroup of  $G$  then the restriction of  $\pi$  to  $K$  is a direct sum of continuous finite-dimensional representations, each isomorphism class occurring with finite multiplicity.

If  $P$  is a minimal parabolic with Levi decomposition  $P = MN$  and modulus character  $\delta = \delta_P$ , and  $(\sigma, U)$  is an admissible representation of  $M$ , then  $\text{Ind}(\sigma|P, G)$  is the right regular representation of  $G$  on the space of all locally constant  $f: G \rightarrow U$  such that  $f(nmg) = \sigma\delta^{\frac{1}{2}}(m)f(g)$  for all  $n \in N$ ,  $m \in M$ ,  $g \in G$ . It is admissible.

A special role is played in the global theory by the unramified representations. If  $G$  is an unramified group - i.e. obtained by base extension to  $k$  from a smooth reductive scheme over  $\text{Spec}(\mathcal{O})$  - then an irreducible admissible representation is said to be unramified if it contains a non-zero vector fixed by the compact open subgroup  $G(\mathcal{O})$ . Any irreducible unramified representation may be embedded into some  $\text{Ind}(\sigma|P, G)$  where  $P$  is minimal and  $\sigma$  is an unramified character of  $M$  (which is a torus by the assumption on  $G$ ).

In contrast to the case where  $k = \mathbb{R}$ , there exist irreducible admissible representations of  $G$  which are contained in no  $\text{Ind}(\sigma|P, G)$  with  $P$  proper. They are called absolutely cuspidal and are also characterized by the property that their matrix coefficients are of compact support modulo  $Z_G$ . They are therefore essentially square-integrable. Given these, however, there is indeed an analogue of Harish-Chandra's result:

2.1.1. Theorem If  $\pi$  is any irreducible admissible representation of  $G$  then there exists a parabolic  $P$  and an absolutely cuspidal  $\sigma$  such that  $\pi$  may be embedded into  $\text{Ind}(\sigma|P, G)$ .

This was first proven by Jacquet [15] for  $\text{GL}_n$ . A very simple proof now exists (see [6]).

The analogue of Proposition 1.2.3 is valid here.

One expects to have for  $p$ -adic  $k$  an analogue of the classification theorem of Langlands [19], but I am not aware that anyone has written down a proof. Nor am I aware, on the other hand, of any point in Langlands' proof that does not go through as easily or even more easily in this case,



so I state here as accomplished results:

2.2.2. Theorem If  $\sigma$  is an irreducible essentially square-integrable representation of  $P$  with  $|\sigma| \in D^+(P)$ , then the image of  $\text{Ind}(\sigma|P, G)$  with respect to  $T_G$  is irreducible.

Call it  $\text{Ind}^+(\sigma)$  as before.

2.2.3. Theorem Every irreducible admissible representation of  $G$  is isomorphic to  $\text{Ind}^+(\sigma|P, G)$  for a unique  $P$  and  $\sigma$ .

In contrast to the archimedean case, every  $p$ -adic reductive group possesses essentially square-integrable representations, and even absolutely cuspidal ones.

2.2. Now let  $G = GL_n(k)$ .

The analogue of Theorem 1.3.1 is also due (as far as I know) to Jacquet and Shalika:

2.2.1. Theorem If  $\sigma$  is an irreducible, square-integrable, admissible representation, then  $\text{Ind}(\sigma)$  is irreducible.

Incidentally, I understand that the proof is similar

to that for  $GL_2$  in [16] - one considers the restriction to a certain maximal proper parabolic subgroup. Jacquet tells me that the proof uses an unpublished result of Bernstein, that every square-integrable representation has a Kirillov model.

The same sort of analysis I used before now goes through to reduce the conjectural classification of representations to the classification of essentially square-integrable representations. (I should mention that the same question as before about  $L$ - and  $\epsilon$ -factors is unanswered in this case also.) The real and  $p$ -adic situations diverge seriously, however. A different form of the conjectural relationship between  $W_k$  and  $GL_n$  is necessary; this is already evident for  $GL_2$ , where one has somehow to deal with the special representations (see [4] , [8] ).

Recall that  $W_k$  is the inverse image in  $Gal(k_s/k)$  of the powers of the Frobenius modulo  $p$ . Let  $Fr$  be some element in  $W_k$  whose image mod  $p$  is in fact the Frobenius. Let  $v$  be the usual norm homomorphism from  $W_k$  to  $k$  (so that, to get things straight,  $Fr$  corresponds to a generator of  $p$ ). Deligne in [9] defines a modified Weil group  $W'_k$ ; it is unimportant to say exactly what it is, but only to say that

a continuous complex representation of  $W_k'$  is a pair  $(\rho, N)$  where (1)  $\rho$  is a continuous complex representation of  $W_k$  and (2)  $N$  is a nilpotent endomorphism of the space of  $\rho$  such that for all  $w$  in  $W_k$  one has  $\rho(w)N\rho(w)^{-1} = |v|(w)N$ . Of course  $N$  may be 0. It is said to be Fr - semi-simple if  $\rho(\text{Fr})$  is semi-simple. (Incidentally, Deligne and Langlands seem to have conceived the idea of introducing these representations independently.)

2.2.2. Conjecture There exists a natural bijective correspondence between the isomorphism classes of indecomposable, continuous, complex, Fr-semi-simple representations of  $W_k'$  of dimension  $n$  and those of irreducible, admissible, essentially square-integrable representations of  $GL_n(k)$ . The irreducible representations of  $W_k$  correspond to the absolutely cuspidal representations of  $GL_n$ .

There is one rather distinguished indecomposable representation of  $W_k'$  of dimension  $n$  which Deligne [8] calls  $Sp(n)$ :

$$w \mapsto \begin{pmatrix} 1 & & & \\ & |v|(w) & & \\ & & \ddots & \\ & & & |v|^{n-1}(w) \end{pmatrix}$$

and

$$N = \begin{pmatrix} 0 & 1 & \dots & 0 \\ & \ddots & \ddots & \\ & & \ddots & \\ & & & 1 \\ & & & & 0 \end{pmatrix}.$$

it plays a fundamental role because of:

2.2.3. Proposition ([8] 3.1.3). The indecomposable, continuous, complex representations of  $W_k$  comprise exactly those of the form  $\rho \otimes \text{Sp}(n)$ , where  $\rho$  is an irreducible, continuous, complex representation of  $W_k$ .

To the representation  $\text{Sp}(n)$  itself corresponds the Steinberg representation of  $\text{GL}_n(k)$ , which is an analogue of the special representation of  $\text{GL}_2$ . It is the unique irreducible quotient of  $\text{Ind}(\sigma|P, G)$ , where  $P$  is the Borel

subgroup of upper triangular matrices and  $\sigma$  is the character  $(1, |v|, \dots, |v|^{n-1}) = \delta_P^{\frac{1}{2}} \otimes |v|^{\frac{1}{2}(n-1)}$  (see [5] and [14]).

Of course,  $n$  may be 1. One would expect something similar to exist for other parabolics; more precisely one might conjecture that

if (1)  $\sigma$  is any irreducible, absolutely cuspidal representation of  $GL_m$ ; (2)  $n = md$  and  $P$  is the parabolic subgroup of  $GL_n$  corresponding to the partition  $(m, \dots, m)$  of  $n$ ; (3)  $\tau = (\sigma, \dots, \sigma \otimes |v|^{n-1})$ ; then there exists a unique irreducible quotient of  $\text{Ind}(\tau|P, G)$ , and it is essentially square-integrable.

At the moment, this seems to be attackable in only a few cases - when  $m = 1$  it is known, and when  $m = 2$  I imagine one can do it - but one elegant idea ought to be able to do all cases at once.

If the above conjecture were known to be true, then Conjecture 2.2.2 would come down to what one really thinks of as its heart, the correspondence between irreducibles and absolutely cuspidals. Of course it is classical for  $n = 1$ . Otherwise, the only situation which is complete is when  $n = 2$  and the residue field characteristic is odd; the

proof is more or less unsatisfactory because it does not give any direct relationship between  $W_k$  and  $GL_2$ . For the case of residue characteristic two and  $GL_2$ , one can presumably at least count the number of representations of each of  $W_k$  and  $GL_2$  with a given conductor (towards this see [23]), but getting the  $\varepsilon$ -factors to coincide seems hopeless.

Deligne in a letter to Piatetskii-Shapiro (see [10]) has managed to use a local theory of elliptic modular schemes to accomplish something when  $k = \mathbb{Q}_p$  (all rational primes  $p$ ) but his results are, as far as I know, incomplete.

In [16] it is shown that the conjecture is true for  $GL_2$  if the Artin conjecture holds for two-dimensional representations of global Galois groups. It is therefore true for the localizations of function fields. Also, it may follow in certain cases from Langlands' recent work on this conjecture.

For  $GL_3$  recent global results in [17] similarly apply. For  $n > 3$ , these tricks give out, and one is very ignorant. Certain representations of  $GL_n$  for all  $n$  have been constructed by Gerardin [12], but the exact relationship with Langlands' conjecture is unclear. They should correspond to the  $n$ -dimensional representations of  $W_k$  one gets by

inducing from the multiplicative group of the unramified extension of degree  $n$ , but matching up  $L$ - and  $\varepsilon$ -factors looks difficult (and there are grounds for believing that the matching may not be the obvious one).

The most fruitful recent idea has been Shintani's ([25] and [26]), which was so suggestive to Langlands in the case of  $GL_2$ . What is most intriguing is the analogy with the classical abelian theory.

### §3. Global fields.

Let  $k$  now be a number field. (I exclude finite characteristic only because it would require separate treatment occasionally.) Let  $A$  be its adèle ring,  $A_f$  the ring of finite adèles (the restricted product of the non-archimedean completions), and  $S_\infty$  the set of archimedean places. Let  $\bar{k}$  be an algebraic closure of  $k$ .

3.1. Let  $G$  be an arbitrary reductive group defined over  $k$ . Let  $G_\infty$  be the product  $\prod G(k_v)$  ( $v \in S_\infty$ ); by restriction of the ground field from  $k$  to  $\mathbb{Q}$ ,  $G_\infty$  is the group of  $\mathbb{R}$ -valued points on a reductive group defined over  $\mathbb{R}$ . Let  $\mathfrak{g}_\infty$  be its Lie algebra, let  $K_v$  for each  $v \in S_\infty$  be a maximal



compact of  $G(k_v)$ , and let  $K_\infty$  be  $\prod K_v$ .

The notion of an admissible representation of  $G(A_f)$  is defined entirely in analogy with that of local groups - to restate it slightly, it is one on a space  $V$  such that (1) the isotropy group of any  $v \in V$  is open and (2) for any given open subgroup  $K$  the subspace  $V^K$  is finite-dimensional.

An admissible representation of  $G(A)$  is a simultaneous representation  $(\pi, V)$  of  $G(A_f)$ ,  $\mathfrak{g}_\infty$ , and  $K_\infty$  such that (1)  $G(A_f)$  commutes with  $\mathfrak{g}_\infty$  and  $K_\infty$ ; (2) for any open  $K$  in  $G(A_f)$  the representation of  $\mathfrak{g}_\infty$  and  $K_\infty$  on  $V^K$  is admissible; (3) for any continuous, finite-dimensional  $K_\infty$ -representation  $\xi$  the space  $\text{Hom}_{K_\infty}(\xi, V)$  is, with the obvious representation of  $G(A_f)$  defined on it, admissible. Any irreducible admissible representation is uniquely factorizable as a restricted tensor product  $\hat{\otimes} \pi_v$  of irreducible admissible representations of the  $G(k_v)$  (§9 of [16]), almost all of which are unramified.

In class field theory one considers characters of the idèle class group  $A^\times/k^\times$ ; generalizing this, one now studies the right regular representation of  $G(A)$  on the spaces of automorphic forms  $A(\epsilon)$  on  $G(k)\backslash G(A)$ . Here  $\epsilon$  is a character of the group  $Z_G(A)/Z_G(k)$ , according to which

$Z_G(A)$  acts on each function in  $A(\varepsilon)$ ; the definition of  $A(\varepsilon)$  for arbitrary  $G$  is the obvious generalization of what it is for  $GL_2$ . Large and essentially continuous families of representations of  $G(A)$  occur in  $A(\varepsilon)$  as representations induced from parabolic subgroups by representations occurring in the spaces of automorphic forms for their reductive components - this is the theory of Eisenstein series. The space of cusp forms  $A_0(\varepsilon)$  is the orthogonal complement of these, and comprises in some sense the atoms of the theory. It is the direct sum of a countable number of irreducible, admissible, essentially unitary representations of  $G(A)$ , and a large part of Langlands' conjectures is concerned with interpreting the constituents arithmetically. This is in analogy with interpreting certain idèle class group characters as those of the Galois group, or attaching them to abelian varieties with complex multiplication. Similarly one expects some, but necessarily all, of the representations in  $A_0(\varepsilon)$  to be related to complex and  $\ell$ -adic representations of Galois and Weil groups. And this in turn is part of an even larger framework in which one links the spaces of automorphic forms for distinct groups, as explained in [18].

3.2. Now let  $G = GL_n$ . As a particular case of the very general ideas mentioned above one expects that

to every irreducible, continuous, complex,  $n$ -dimensional representation  $\rho$  of  $\text{Gal}(\bar{k}/k)$  corresponds a constituent  $\pi(\rho)$  of the space  $A_0(\epsilon)$  for some  $\epsilon$ . More precisely, the character  $\epsilon$  is the character of  $A^\times/k^\times$  corresponding to  $\det(\rho)$  by local class field theory, and the local factors of  $\pi(\rho)$  should be those determined by the local Galois representations associated to  $\rho$ .

Reducible representations of the Galois group, incidentally, should correspond to automorphic forms arising from Eisenstein series.

For  $n = 2$  or  $3$  this follows from the Artin conjecture on the entire-ness of  $L$ -functions attached to  $\rho$  and its twistings by characters, so that it is true in particular when  $\rho$  is induced from an idèle class group character of a quadratic or cubic extension of  $k$  ([16] and [17]). But of course what one really wants to do is obtain Artin's conjecture as a consequence of representation theory (a program begun in [20]). At this point it is not at all clear how far-reaching the Langlands-Saito-Shintani lifting theory will

go, but it seems promising.

In [24] it is at least shown that constituents of  $A_0(\epsilon)$  occur with multiplicity one.

#### §4. $\underline{GL_2(\mathbb{Q})}$

4.1. Let

$$G = GL_2(\mathbb{R})$$

$P$  = the parabolic subgroup of upper  
triangular matrices

$A$  = diagonal matrices

$Z$  = scalar matrices

$K = SO(2)$  (later on I shall call it  $K_\infty$ )

$$\alpha = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

The element  $\alpha$  normalizes  $K$ , taking  $k$  to  $k^{-1}$ , and the two together generate the maximal compact  $O(2)$ .

Let  $C$  be the standard Casimir element of the enveloping algebra (which is  $1/2$  that in Jacquet-Langlands).

If  $\rho$  is a reducible, unitary, two-dimensional representation of  $W_{\mathbb{R}}$  with  $\det \rho = 1$ , then it is the direct sum of a character  $\chi$  and its inverse and there exists  $\tau \in \mathbb{R}$ ,  $m = 0$

or 1 such that  $\chi(x) = |x|^{i\tau}(\text{sgn } x)^m$ . If  $\rho$  is trivial on  $W_{\mathbb{C}}$  - i.e. if it is essentially a representation of  $\text{Gal}(\mathbb{C}/\mathbb{R})$  - then  $\tau = 0$ . The representation  $\pi(\rho)$  of  $\text{GL}_2(\mathbb{R})$  is the unitary principal series  $\text{Ind}(\sigma|P, G)$ , where  $\sigma = (\chi, \chi^{-1})$ .

4.1.1. Proposition The representation  $\text{Ind}(\sigma)$  is the unique irreducible admissible representation  $(\pi, V)$  of  $\text{GL}_2(\mathbb{R})$  such that

- (a) There exists  $v \neq 0$  in  $V$  which is fixed by all  $k \in K$  and such that  $\pi(\alpha)v = (-1)^m v$ ;
- (b)  $\pi(C) = -1/4 (1 + \tau^2)$  ;
- (c) The restriction of  $\pi$  to  $Z$  is trivial.

The proof is easy enough to get out of the discussion on  $\text{GL}_2(\mathbb{R})$  in [16].

4.2. Let  $H$  be the Poincaré upper half-plane, on which  $G^{\text{pos}} = \text{GL}_2^{\text{pos}}(\mathbb{R})$  acts in the usual way. The Laplacian on  $H$  with respect to the  $G^{\text{pos}}$ -invariant metric  $ds^2 = (dx^2 + dy^2)/y^2$  is

$$\Delta = y^2(\partial^2/\partial x^2 + \partial^2/\partial y^2)$$

and is of course also  $G^{\text{pos}}$ -invariant.

Let  $\Gamma$  be a discrete subgroup of  $G^{\text{pos}}$  such that  $\Gamma \backslash H$  has finite area. For every  $\lambda \in \mathbb{C}$  define the space  $M(\lambda, \Gamma)$  to be that of all  $f: H \rightarrow \mathbb{C}$  such that

$$(M1) \quad f \cdot \gamma = f \text{ for all } \gamma \in \Gamma;$$

$$(M2) \quad \Delta f = \lambda f ;$$

$$(M3) \quad f \text{ has moderate growth at all cusps of } \Gamma.$$

The subspace  $S(\lambda, \Gamma)$  of cuspidal forms is that of all  $f$  satisfying in addition

$$(M4) \quad f \text{ is rapidly decreasing at all cusps of } \Gamma.$$

Using the obvious inner product on  $S(\lambda, \Gamma)$  one can see without too much trouble that this space is trivial unless  $\lambda$  is real and  $\leq 0$ , and that if  $\lambda = 0$  then it contains only the constants.

If  $f$  is any function on  $H$  satisfying (M2) and the equation

$$f(z + N) = f(z)$$

for all  $z \in H$ , where  $N$  is some real positive number, then it has a Fourier expansion

$$f(x + iy) = \sum_{n \in \mathbb{Z}} \phi_n(y) e^{2\pi i n x / N}.$$

The function  $\phi_n$  satisfies the differential equation

$$\phi'' - \left( 4\pi^2 n^2 / N^2 + \frac{\lambda}{y^2} \right) \phi = 0.$$

If  $n = 0$ , this is Euler's equation. It has the general solution

$$c_1 y^{t_1} + c_2 y^{t_2}$$

if the roots of the indicial equation  $t(t - 1) - \lambda = 0$  are distinct and equal to  $t_1$  and  $t_2$ , and the general solution

$$c_1 y^{1/2} + c_2 y^{1/2} \log y$$

if  $\lambda = -1/4$  so that this equation has equal roots.

If  $n \neq 0$  then one may change variables to  $Y = 4\pi|n|y/N$  to obtain the equation

$$\Phi'' - \left(1 + \frac{\lambda}{Y^2}\right) \Phi = 0.$$

The theory of irregular singularities (see Chapter 4 of [3] for example) says that there are two solutions  $\Phi_\lambda$  and  $\Psi_\lambda$  of this equation with the asymptotic behaviour

$$\Phi_\lambda(Y) \sim e^{-Y}, \quad \Psi_\lambda(Y) \sim e^Y$$

as  $Y \rightarrow \infty$ . (In fact  $\Phi_\lambda$  and  $\Psi_\lambda$  are of the form  $y^{1/2} J_\lambda$  where  $J_\lambda$  is a solution of a modified Bessel's equation, but that won't play a role here.) If  $i\infty$  is a cusp of  $\Gamma$  then (M3) for this cusp means that no  $\Psi_\lambda$  appears in the Fourier expansion, and (M4) means that in addition the term for  $n = 0$  vanishes. Any other cusp may be transformed to  $i\infty$  and dealt



with accordingly.

These spaces were all first defined, I believe, by Maass in [22], where he proved among other things that they are finite-dimensional.

Assume now that  $\Gamma$  is a subgroup of  $GL_2(\mathbb{Q})$ . Let  $A$  be the adèles of  $\mathbb{Q}$ ,  $K_f$  a compact open subgroup of  $GL_2(A_f)$  such that  $K_f \cap GL_2^{\text{pos}}(\mathbb{Q}) = \Gamma$  and  $\det K_f = \prod \mathbb{Z}_p^\times$ . For  $f \in M(\lambda, \Gamma)$  define the function  $F$  on  $GL_2(A)$ :

$$F(g_0 g_\infty g_f) = f(g_\infty(i))$$

for  $g_0 \in GL_2(\mathbb{Q})$ ,  $g_\infty \in GL_2^{\text{pos}}(\mathbb{R})$ ,  $g_f \in K_f$  (recall that because of strong approximation and class number one for  $\mathbb{Q}$ ,  $GL_2(A)$  is the product of these three groups). The function  $F$  satisfies

$$(A1) \quad L(g_0)F = F \text{ for all } g_0 \in GL_2(\mathbb{Q}) ;$$

$$(A2) \quad R(k)F = F \text{ for all } k \in K_\infty \times K_f ;$$

$$(A3) \quad R(z)F = F \text{ for all } z \text{ scalar and real} ;$$

$$(A4) \quad R(C)F = \lambda F ;$$

$$(A5) \quad F \text{ is of moderate growth on } GL_2(A) \text{ (see pp.}$$

329-30 of [16]).

These properties in fact characterize the image of  $M(\lambda, \Gamma)$ , and the image of  $S(\lambda, \Gamma)$  is characterized by these together with the appropriate strengthening of (A5).

Assume that  $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  normalizes  $\Gamma$  and  $K_f$ . Then the map  $z \mapsto -\bar{z}$  induces an isometry of  $\Gamma \backslash H$ , hence a linear automorphism of  $M(\lambda, \Gamma)$ . This space is therefore the direct sum of the eigenspaces  $M^m(\lambda, \Gamma)$  ( $m = 0, 1$ ) on which this automorphism acts as  $(-1)^m$ . Similarly for  $S(\lambda, \Gamma)$ . The image of  $M^m(\lambda, \Gamma)$  with respect to the map  $f \mapsto F$  defined above is determined by the condition

$$(A6) \quad R(\alpha)F = (-1)^m F,$$

where  $\alpha$  is still considered an element of  $GL_2(\mathbb{R})$ .

For each irreducible constituent  $(\pi, V)$  of the space of cusp forms on  $GL_2(A)$ , let  $S^m(\pi, \lambda, \Gamma)$  be the inverse image in  $S^m(\lambda, \Gamma)$ . If  $\pi = \pi_\infty \otimes \pi_f$ , then in order for  $S^m(\pi, \lambda, \Gamma)$  to be non-trivial it is necessary and sufficient that  $\pi_\infty$  satisfy the conditions (1) there exists  $v \neq 0$  in  $V_\infty$  fixed by all  $k \in K_\infty$  such that  $\pi(\alpha)v = (-1)^m v$ ; (2)  $\pi(C) = \lambda$ ; (3)  $\pi|_{Z_\infty}$  is trivial, and  $\pi_f$  satisfy the condition that  $V_f^{K_f} \neq 0$ . Under these circumstances,  $S^m(\pi, \lambda, \Gamma) \cong V_f^{K_f}$ .

4.3. Let  $\rho$  be an irreducible two-dimensional representation of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  such that

$$\rho(\tau) \sim \begin{pmatrix} (-1)^m & 0 \\ 0 & (-1)^m \end{pmatrix}$$

(recall that  $\tau$  is complex conjugation in  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ , and is determined up to conjugacy). Let  $N$  be the Artin conductor of  $\rho$  and

$$L(s, \rho) = \sum a_n n^{-s}$$

its L-function. Define a function  $f_\rho$  on  $H$ :

$$f_\rho(x + iy) = \sum_{n>0} \frac{(\text{sgn } n)^m a_n |n|}{\sqrt{|n|}} \phi_{-1/4}(4\pi |n| y) e^{2\pi i n x}.$$

All the above considerations imply that as a special case of Langlands' global conjectures one has:

4.3.1. Conjecture. The function  $f$  lies in  $S^m(-1/4, \Gamma_1(N))$ .

This is true if and only if the Artin conjecture holds for all the representations  $\rho \otimes \chi$ , where  $\chi$  ranges over all the Dirichlet characters. More generally, one might hope that in fact all primitive forms in  $S^m(-1/4, \Gamma_1(N))$  are obtained in this way. This would be the result analogous to that of Deligne-Serre for these forms. But the techniques applied by Deligne-Serre do not seem likely to work here, and this seems far out of reach.

## REFERENCES

1. A. Borel, Représentations de Groupes Localements Compacts, Springer Lecture Notes No. 276, 1972.
2. ———, Formes automorphes et séries de Dirichlet (d'après R.P. Langlands), Séminaire Bourbaki, June, 1975.
3. F. Brauer and J. Nohel, Ordinary Differential Equations, Benjamin, New York, 1967.
4. W. Casselman, On representations of  $GL_2$  and the arithmetic of modular curves, in the Proceedings of the International School on Modular Functions, Springer Lecture Notes No. 349, 1973.
5. ———, On a p-adic vanishing theorem of Garland, Bull. Amer. Math. Soc., 80 (1974), 1001 - 1004.
6. ———, Introduction to the theory of admissible representations of p-adic reductive groups, to appear.
7. ———, Matrix coefficients of admissible representations, to appear.
8. P. Deligne, Formes modulaires et représentations de  $GL(2)$ , in Springer Lecture Notes No. 349, 1973.
9. ———, Les constantes des equations fonctionnelles des fonctions L, in Springer Lecture Notes No. 349, 1973.
10. ———, a letter to Piatetskii-Shapiro published in Russian in Matematika - Period. Sb. Perevedov Inostran. Statei 18 (1974), 110-112.
11. M. Duflo, Lecture notes on representations of complex semi-simple groups, Paris, 1974.
12. P. Gerardin, Construction de Séries Discretes p-adiques, Springer Lecture Notes No. 462, 1975.

13. I.M. Gelfand and D. Kazhdan, Representations of the group  $GL(n, K)$ , in Proceedings of the Summer School of the Bolyai Janos Math. Soc. on Group Representations, Adam Hilger, London, 1975.
14. R. Godement and H. Jacquet, Zeta Functions of Simple Algebras, Springer Lecture Notes No. 260, 1972.
15. H. Jacquet, Représentations des groupes linéaires p-adiques, in Theory of Group Representations and Fourier Analysis, Edizioni Cremonese, Rome, 1971.
16. \_\_\_\_\_, and R.P. Langlands, Automorphic Forms on  $GL(2)$ , Springer Lecture Notes No. 114, 1970.
17. \_\_\_\_\_, I. I. Piatetskii-Shapiro, and J. Shalika, A converse theorem for  $GL(3)$ , to appear.
18. R.P. Langlands, Problems in the theory of automorphic forms, in Springer Lecture Notes No. 170, 1970.
19. \_\_\_\_\_, On the classification of irreducible representations of real reductive groups, notes from the Institute for Advanced Study, Princeton, 1974.
20. \_\_\_\_\_, Base change for  $GL(2)$ , notes from I. A. S., 1975.
21. J. Lepowsky and N. Wallach, Finite- and infinite-dimensional representations of linear semi-simple groups, Trans. Amer. Math. Soc. 184 (1973), 223-246.
22. H. Maass, Über eine neue Art ... , Math. Ann. 121 (1944).
23. A. Nobs and J. Wolfart, Les représentations irréductibles du groupe  $SL_2(\mathbb{Z}_2)$ , C. R. Acad. Sc. Paris, t. 281, 261-64.
24. J. Shalika, The multiplicity one theorem for  $GL_n$ , Ann. of Math., 100 (1974), 171-193.

25. T. Shintani, On liftings of holomorphic forms, in the Proceedings of the 1975 U. S. - Japan Seminar on application of automorphic forms to number theory, Ann Arbor, 1975.
26. \_\_\_\_\_, Two remarks on irreducible characters of finite general linear groups, to appear.
27. G. Warner, Harmonic Analysis on Semi-simple Groups, Vol. I, Springer, New York, 1972.